

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開平11-53264

(43) 公開日 平成11年(1999) 2月26日

(51) Int.Cl. ⁶	識別記号	F I	
G 0 6 F 12/14	3 2 0	G 0 6 F 12/14	3 2 0 E 3 2 0 B
G 1 1 B 20/10		G 1 1 B 20/10	H
H 0 4 L 9/08		H 0 4 L 9/00	6 0 1 E 6 0 1 A

審査請求 未請求 請求項の数34 O L (全 45 頁)

(21) 出願番号	特願平9-210899	(71) 出願人	000002185 ソニー株式会社 東京都品川区北品川6丁目7番35号
(22) 出願日	平成9年(1997) 8月5日	(72) 発明者	石黒 隆二 東京都品川区北品川6丁目7番35号 ソニ ー株式会社内
(31) 優先権主張番号	特願平9-106104	(72) 発明者	大澤 義知 東京都品川区北品川6丁目7番35号 ソニ ー株式会社内
(32) 優先日	平9(1997) 4月23日	(72) 発明者	刑部 義雄 東京都品川区北品川6丁目7番35号 ソニ ー株式会社内
(33) 優先権主張国	日本 (J P)	(74) 代理人	弁理士 稲本 義雄
(31) 優先権主張番号	特願平9-143699		
(32) 優先日	平9(1997) 6月2日		
(33) 優先権主張国	日本 (J P)		

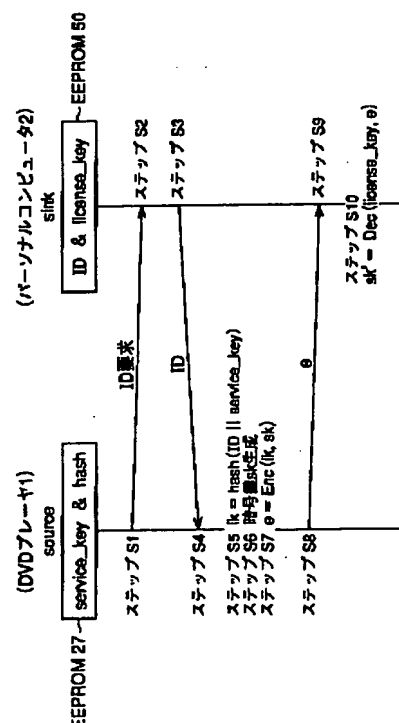
最終頁に続く

(54) 【発明の名称】 情報処理装置および方法、情報処理システム、並びに提供媒体

(57) 【要約】

【課題】 情報の不正なコピーを防止する。

【解決手段】 ソースとしてのDVDプレーヤ1のEEPROM 27に、hash関数とservice_keyを記憶しておく。シンクとしてのパーソナルコンピュータ2のEEPROM 50には、そのIDとlicense_keyを記憶しておく。ステップS1において、DVDプレーヤ1は、パーソナルコンピュータ2に対してIDを要求する。IDの供給を受けたとき、DVDプレーヤ1は、IDとservice_keyを連結して得られるデータ (ID || service_key) に対してhash関数を適用し、キーlkを得る。さらに、暗号鍵skを生成し、これを鍵lkを鍵として暗号化したデータeをパーソナルコンピュータ2に伝送する。パーソナルコンピュータ2は、この暗号化データeをlicense_keyを鍵として復号し、暗号鍵skと等しい暗号鍵sk'を得る。



【特許請求の範囲】

【請求項1】 自分自身に固有の識別データと、他の情報処理装置から伝送されてきた所定の情報に所定の処理を施すことに対する許可に対応する第1のキーLKを記憶する記憶手段と、

所定の情報に対して許可された処理を行う処理手段とを備え、

前記第1のキーLKは、前記識別データと、所定の処理を施す前記情報に対応する第2のキーSVKに基づいて生成されていることを特徴とする情報処理装置。

【請求項2】 前記第1のキーLKを用いて、前記他の情報処理装置から伝送されてきた暗号化されている第3のキーSKを復号するキー復号手段をさらに備えることを特徴とする請求項1に記載の情報処理装置。

【請求項3】 前記第3のキーSKを用いて、前記他の情報処理装置から伝送されてくる暗号化されている情報を復号する情報復号手段をさらに備えることを特徴とする請求項2に記載の情報処理装置。

【請求項4】 前記第3のキーSKは、1つのセッションにおいて不変の第4のキーSSと、前記セッション内において変更される第5のキーSiとにより構成されていることを特徴とする請求項3に記載の情報処理装置。

【請求項5】 伝送されてきた情報を復号する乱数を生ずる乱数発生手段と、

前記第4のキーSS、または前記乱数発生手段により発生された乱数で復号された情報を用いて、前記乱数発生手段が乱数を生ずるときの初期値を演算する演算手段とをさらに備えることを特徴とする請求項4に記載の情報処理装置。

【請求項6】 前記記憶手段は、複数の前記第1のキーLKを記憶し、

前記キー復号手段は、前記他の情報処理装置から伝送されてきた、複数の前記第1のキーLKの中から、前記情報を識別する情報識別データに対応する前記第1のキーLKを選択し、前記第3のキーSKを復号することを特徴とする請求項2に記載の情報処理装置。

【請求項7】 前記キー復号手段は、認証を行うためのソフトウェアプログラムにより構成されていることを特徴とする請求項2に記載の情報処理装置。

【請求項8】 前記キー復号手段は、前記キーを用いて暗号化されて伝送されたデータを復号化するためのハードウェアにより構成されていることを特徴とする請求項2に記載の情報処理装置。

【請求項9】 前記他の情報処理装置から前記識別データの伝送の要求があったとき、前記識別データを前記他の情報処理装置に伝送する伝送手段をさらに備えることを特徴とする請求項1に記載の情報処理装置。

【請求項10】 前記第1のキーLKを、所定の関数を用いて更新する更新手段をさらに備えることを特徴とする請求項1に記載の情報処理装置。

【請求項11】 前記他の情報処理装置から伝送されてきた、暗号化されている情報を前記第3のキーSKを用いて復号した結果に対応して、前記第1のキーLKを更新する更新手段をさらに備えることを特徴とする請求項3に記載の情報処理装置。

【請求項12】 自分自身に固有の識別データと、他の情報処理装置から伝送されてきた所定の情報に所定の処理を施すことに対する許可に対応する第1のキーLKを記憶する記憶ステップと、

所定の情報に対して許可された処理を行う処理ステップとを備え、

前記第1のキーLKは、前記識別データと、所定の処理を施す前記情報に対応する第2のキーSVKに基づいて生成されていることを特徴とする情報処理方法。

【請求項13】 自分自身に固有の識別データと、他の情報処理装置から伝送されてきた所定の情報に所定の処理を施すことに対する許可に対応する第1のキーLKを記憶する記憶ステップと、

所定の情報に対して許可された処理を行う処理ステップとを備え、

前記第1のキーLKは、前記識別データと、所定の処理を施す前記情報に対応する第2のキーSVKに基づいて生成されているプログラムを提供することを特徴とする提供媒体。

【請求項14】 他の情報処理装置に伝送する情報に対応する第1のキーSVKと、所定の関数を記憶する記憶手段と、

前記他の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信手段と、

前記識別データと前記第1のキーSVKに対して前記関数を適用し、第2のキーLKを生成する第1の生成手段と、

第3のキーSKを生成する第2の生成手段と、

前記第2のキーLKを用いて、前記第3のキーSKを暗号化し、前記他の情報処理装置に伝送する暗号化手段とを備えることを特徴とする情報処理装置。

【請求項15】 前記第2のキーLKを、前記所定の関数を用いて更新する更新手段をさらに備えることを特徴とする請求項14に記載の情報処理装置。

【請求項16】 前記他の情報処理装置に対して、前記暗号化手段により暗号化されたデータを既に送信したか否かを判定する判定手段をさらに備えることを特徴とする請求項14に記載の情報処理装置。

【請求項17】 前記受信手段は、さらに、前記他の情報処理装置から認証の要求を受信し、

前記記憶手段は、さらに、前記他の情報処理装置がバスを介して通信を行う上において割り当てられている割り当て番号を記憶することを特徴とする請求項14に記載の情報処理装置。

【請求項18】 他の情報処理装置に伝送する情報に対応する第1のキーSVKと、所定の関数を記憶する記憶ス

テップと、
前記他の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信ステップと、
前記識別データと前記第1のキーSVKに対して前記関数を適用し、第2のキーLKを生成する第1の生成ステップと、
第3のキーSKを生成する第2の生成ステップと、
前記第2のキーLKを用いて、前記第3のキーSKを暗号化し、前記他の情報処理装置に伝送する暗号化ステップとを備えることを特徴とする情報処理方法。

【請求項19】 他の情報処理装置に伝送する情報に対応する第1のキーSVKと、所定の関数を記憶する記憶ステップと、
前記他の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信ステップと、
前記識別データと前記第1のキーSVKに対して前記関数を適用し、第2のキーLKを生成する第1の生成ステップと、
第3のキーSKを生成する第2の生成ステップと、
前記第2のキーLKを用いて、前記第3のキーSKを暗号化し、前記他の情報処理装置に伝送する暗号化ステップとを備えるプログラムを提供することを特徴とする提供媒体。

【請求項20】 第1の情報処理装置と第2の情報処理装置とにより構成される情報処理システムにおいて、
前記第1の情報処理装置は、
前記第2の情報処理装置に伝送する情報に対応する第1のキーSVKと、所定の関数を記憶する第1の記憶手段と、
前記第2の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信手段と、
前記識別データと前記第1のキーSVKに対して前記関数を適用し、第2のキーLK1を生成する第1の生成手段と、
第3のキーSK1を生成する第2の生成手段と、
前記第2のキーLK1を用いて、前記第3のキーSK1を暗号化し、前記第2の情報処理装置に伝送する暗号化手段とを備え、
前記第2の情報処理装置は、
自分自身に固有の前記識別データと、所定の情報に所定の処理を施すことに対する許可に対応する第4のキーLK2を記憶する第2の記憶手段と、
前記第4のキーLK2を用いて、前記第1の情報処理装置から伝送を受けた、暗号化されている前記第3のキーSK1を復号する復号手段とを備えることを特徴とする情報処理システム。

【請求項21】 第1の情報処理装置と第2の情報処理装置とにより構成される情報処理システムの情報処理方法において、
前記第1の情報処理装置は、

前記第2の情報処理装置に伝送する情報に対応する第1のキーSVKと、所定の関数を記憶する第1の記憶ステップと、
前記第2の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信ステップと、
前記識別データと前記第1のキーSVKに対して前記関数を適用し、第2のキーLK1を生成する第1の生成ステップと、
第3のキーSK1を生成する第2の生成ステップと、
前記第2のキーLK1を用いて、前記第3のキーSK1を暗号化し、前記第2の情報処理装置に伝送する暗号化ステップとを備え、
前記第2の情報処理装置は、
自分自身に固有の前記識別データと、所定の情報に所定の処理を施すことに対する許可に対応する第4のキーLK2を記憶する記憶ステップと、
前記第4のキーLK2を用いて、前記第1の情報処理装置から伝送を受けた、暗号化されている前記第3のキーSK1を復号する復号ステップとを備えることを特徴とする情報処理方法。

【請求項22】 第1の情報処理装置と第2の情報処理装置とにより構成される情報処理システムの、前記第1の情報処理装置を制御する第1のプログラムと、前記第2の情報処理装置を制御する第2のプログラムとを提供する提供媒体において、
前記第1のプログラムは、
前記第2の情報処理装置に伝送する情報に対応する第1のキーSVKと、所定の関数を記憶する第1の記憶ステップと、
前記第2の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信ステップと、
前記識別データと前記第1のキーSVKに対して前記関数を適用し、第2のキーLK1を生成する第1の生成ステップと、
第3のキーSK1を生成する第2の生成ステップと、
前記第2のキーLK1を用いて、前記第3のキーSK1を暗号化し、前記第2の情報処理装置に伝送する暗号化ステップとを備え、
前記第2のプログラムは、
自分自身に固有の前記識別データと、所定の情報に所定の処理を施すことに対する許可に対応する第4のキーLK2を記憶する記憶ステップと、
前記第4のキーLK2を用いて、前記第1の情報処理装置から伝送を受けた、暗号化されている前記第3のキーSK1を復号する復号ステップとを備えることを特徴とする提供媒体。

【請求項23】 第1のキーLk、第2のキーLk'、および所定の関数Gを記憶する記憶手段と、
他の情報処理装置から伝送されてきた所定の情報に対して許可された処理を行う処理手段とを備え、

前記第2のキーLK'は、前記第1のキーLKと、前記関数Gの逆関数 G^{-1} に基づいて生成されていることを特徴とする情報処理装置。

【請求項24】 擬似乱数を発生する擬似乱数発生手段をさらに備え、
前記記憶手段は、自分自身に固有の識別データをさらに記憶することを特徴とする請求項23に記載の情報処理装置。

【請求項25】 前記第2のキーLK'は、前記識別データと、所定の処理を施す前記情報に対応する第3のキーSVKに基づいて生成されているデータHを、前記擬似乱数発生手段に適用して得られる擬似乱数PRNG(H)と、前記第1のキーLKを前記擬似乱数発生手段に適用して得られる擬似乱数PRNG(LK)に基づいて生成されるデータRを、前記逆関数 G^{-1} に適用して生成されていることを特徴とする請求項24に記載の情報処理装置。

【請求項26】 前記他の情報処理装置から伝送されてきた、前記擬似乱数PRNG(H)を用いて暗号化されている第4のキーSKを、前記第2のキーLK'を前記関数Gに適用して得られるデータG(LK')と、前記擬似乱数PRNG(LK)を用いて復号するキー復号手段をさらに備えることを特徴とする請求項25に記載の情報処理装置。

【請求項27】 第1のキーLK、第2のキーLK'、および所定の関数Gを記憶する記憶ステップと、
他の情報処理装置から伝送されてきた所定の情報に対して許可された処理を行う処理ステップとを備え、
前記第2のキーLK'は、前記第1のキーLKと、前記関数Gの逆関数 G^{-1} に基づいて生成されていることを特徴とする情報処理方法。

【請求項28】 第1のキーLK、第2のキーLK'、および所定の関数Gを記憶する記憶ステップと、
他の情報処理装置から伝送されてきた所定の情報に対して許可された処理を行う処理ステップとを備え、
前記第2のキーLK'は、前記第1のキーLKと、前記関数Gの逆関数 G^{-1} に基づいて生成されているプログラムを提供することを特徴とする提供媒体。

【請求項29】 他の情報処理装置に伝送する情報に対応する第1のキーSVKと、所定の関数を記憶する記憶手段と、
前記他の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信手段と、
第2のキーSKを生成する生成手段と、
擬似乱数を発生する擬似乱数発生手段と、
前記識別データと前記第1のキーSVKに対して前記関数を適用して得られるデータHを、前記擬似乱数発生手段に適用して得られる擬似乱数PRNG(H)を用いて、前記第2のキーSKを暗号化し、前記他の情報処理装置に伝送する暗号化手段とを備えることを特徴とする情報処理装置。

【請求項30】 他の情報処理装置に伝送する情報に

応する第1のキーSVKと、所定の関数を記憶する記憶ステップと、
前記他の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信ステップと、
第2のキーSKを生成する生成ステップと、
擬似乱数を発生する擬似乱数発生ステップと、
前記識別データと前記第1のキーSVKに対して前記関数を適用して得られるデータHを、前記擬似乱数発生ステップに適用して得られる擬似乱数PRNG(H)を用いて、前記第2のキーSKを暗号化し、前記他の情報処理装置に伝送する暗号化ステップとを備えることを特徴とする情報処理方法。

【請求項31】 他の情報処理装置に伝送する情報に対応する第1のキーSVKと、所定の関数を記憶する記憶ステップと、
前記他の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信ステップと、
第2のキーSKを生成する生成ステップと、
擬似乱数を発生する擬似乱数発生ステップと、
前記識別データと前記第1のキーSVKに対して前記関数を適用して得られるデータHを、前記擬似乱数発生ステップに適用して得られる擬似乱数PRNG(H)を用いて、前記第2のキーSKを暗号化し、前記他の情報処理装置に伝送する暗号化ステップとを備えるプログラムを提供することを特徴とする提供媒体。

【請求項32】 第1の情報処理装置と第2の情報処理装置とにより構成される情報処理システムにおいて、
前記第1の情報処理装置は、
前記第2の情報処理装置に伝送する情報に対応する第1のキーSVKと、第1の関数hを記憶する第1の記憶手段と、
前記第2の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信手段と、
第2のキーSKを生成する生成手段と、
擬似乱数を発生する擬似乱数発生手段と、
前記識別データと前記第1のキーSVKに対して前記関数hを適用して得られるデータHを、前記擬似乱数発生手段に適用して得られる擬似乱数PRNG(H)を用いて、前記第2のキーSKを暗号化し、前記第2の情報処理装置に伝送する暗号化手段とを備え、
前記第2の情報処理装置は、
第3のキーLK、第4のキーLK'、および所定の関数Gを記憶する第2の記憶手段と、
前記第1の情報処理装置から伝送されてきた所定の情報に対して許可された処理を行う処理手段とを備え、
前記第4のキーLK'は、前記第3のキーLKと、前記関数Gの逆関数 G^{-1} に基づいて生成されていることを特徴とする情報処理システム。

【請求項33】 第1の情報処理装置と第2の情報処理装置とにより構成される情報処理システムの情報処理方

法において、

前記第1の情報処理装置は、

前記第2の情報処理装置に伝送する情報に対応する第1のキーSVKと、所定の関数 h を記憶する第1の記憶ステップと、

前記第2の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信ステップと、第2のキーSKを生成する生成ステップと、

疑似乱数を発生する疑似乱数発生ステップと、前記識別データと前記第1のキーSVKに対して前記関数 h を適用して得られるデータ H を、前記疑似乱数発生ステップに適用して得られる疑似乱数 $\text{PRNG}(H)$ を用いて、前記第2のキーSKを暗号化し、前記第2の情報処理装置に伝送する暗号化ステップとを備え、

前記第2の情報処理装置は、

第3のキーLk、第4のキーLk'、および所定の関数 G を記憶する第2の記憶ステップと、前記第1の情報処理装置から伝送されてきた所定の情報に対して許可された処理を行う処理ステップとを備え、前記第4のキーLk'は、前記第3のキーLkと、前記関数 G の逆関数 G^{-1} に基づいて生成されていることを特徴とする情報処理方法。

【請求項34】 第1の情報処理装置と第2の情報処理装置とにより構成される情報処理システムの、前記第1の情報処理装置を制御する第1のプログラムと、前記第2の情報処理装置を制御する第2のプログラムを提供する提供媒体において、

前記第1のプログラムは、

前記第2の情報処理装置に伝送する情報に対応する第1のキーSVKと、所定の関数 h を記憶する第1の記憶ステップと、

前記第2の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信ステップと、第2のキーSKを生成する生成ステップと、

疑似乱数を発生する疑似乱数発生ステップと、前記識別データと前記第1のキーSVKに対して前記関数 h を適用して得られるデータ H を、前記疑似乱数発生ステップに適用して得られる疑似乱数 $\text{PRNG}(H)$ を用いて、前記第2のキーSKを暗号化し、前記第2の情報処理装置に伝送する暗号化ステップとを備え、

前記第2のプログラムは、

第3のキーLk、第4のキーLk'、および所定の関数 G を記憶する第2の記憶ステップと、

前記第1の情報処理装置から伝送されてきた所定の情報に対して許可された処理を行う処理ステップとを備え、前記第4のキーLk'は、前記第3のキーLkと、前記関数 G の逆関数 G^{-1} に基づいて生成されていることを特徴とする提供媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、情報処理装置および方法、情報処理システム、並びに提供媒体に関し、特に、より安全にデータを授受することができるようにした、情報処理装置および方法、情報処理システム、並びに提供媒体に関する。

【0002】

【従来の技術】最近、AV機器やパーソナルコンピュータなどの電子機器を、例えばIEEE 1394シリアルバスを介して相互に接続し、相互の間でデータを授受することができるようにするシステムが提案されている。

【0003】このようなシステムにおいて、例えば一般のユーザが、DVDプレーヤにより再生出力された映画情報を、1394シリアルバスを介してモニタに出力し、表示させる行為は、一般的に、DVD（ディスク）を購入した時点において、映画情報の著作権者から許容されているものとされる。しかしながら、DVDプレーヤから再生された映画情報を、光磁気ディスク、その他の記録媒体に記録する行為は、著作権者からの特別な許諾が必要となる。このような場合、例えば、光磁気ディスク装置に、映画情報を記録することが許可されているか否かを表すキーを記憶しておき、このキーを利用して、その光磁気ディスク装置が正当な装置（著作権者からのライセンスを受けた装置）であるか否かを認証するようにし、正当な装置として認証された場合には、その光磁気ディスク装置に映画情報の記録を許容するようにすることが考えられる。

【0004】このような場合、映画情報を伝送する側の装置（以下、このような装置をソース（source）と称する）と、伝送を受けた装置（以下、このような装置をシンク（sink）と称する）との間で、相手側の装置が適正な装置であるか否かを認証する必要がある。

【0005】図41は、このような認証を行う従来の方法を表している。同図に示すように、ソースとシンクは、それぞれ著作権者から予め所定の関数 f を受け取り、それぞれのメモリに記憶しておく。この関数 f は、その入力と出力から、その関数 f を特定するのが困難な関数であり、また、知らないものが、その関数 f に対して任意の入力を与えた場合に得られる出力を推定するのが困難な関数とされる。そして、この関数 f は、著作権者から許可された装置にのみ与えられ、記憶される。

【0006】ソースは乱数 r を発生し、これを1394バスを介してシンクに伝送する。また、ソースは、関数 f に対して乱数 r を適用して、 $x (= f(r))$ を生成する。

【0007】一方、シンク側においては、ソース側から転送されてきた乱数 r を関数 f に適用して、 $y (= f(r))$ を生成する。そして、この y をソース側に伝送する。

【0008】ソース側においては、演算により求めた x と、シンク側から伝送されてきた y を比較し、両者が一

致するか否か ($x=y$ であるか否か) を判定する。両者が一致していれば、ソース側は、シンク側を正当な装置であると認証し、映画情報を所定のキーで暗号化して、シンク側に伝送する。

【0009】このキーとしては、シンクが伝送してきた y を関数 f に適用して生成した値 $k (= f(y))$ が用いられる。シンク側においても、同様にして、 y に関数 f を適用して、キー $k (= f(y))$ を生成する。そして、このキー k を用いて、ソース側から伝送されてきた、暗号化されている映画データを復号する。

【0010】

【発明が解決しようとする課題】しかしながら、このような方法においては、ソースまたはシンクとして、データを授受するすべての電子機器が、同一の関数 f を秘密裡に保持する必要がある。

【0011】その結果、例えば、不正なユーザによって、1つの電子機器に保持されている関数 f が盗まれてしまったような場合、この不正なユーザは、1394バスを介して授受されるデータを監視することにより、鍵 k を生成することができ、暗号化されているデータを解読することが可能となる。その結果、不正なユーザは、所望の電子機器になりすまして、不正に情報を盗むことが可能となる。

【0012】本発明はこのような状況に鑑みてなされたものであり、暗号または復号に必要な情報が盗まれたとしても、不正なユーザが、これを用いて所望の電子機器になりすますことができないようし、より安全性を図るようにするものである。

【0013】

【課題を解決するための手段】請求項1に記載の情報処理装置は、自分自身に固有の識別データと、他の情報処理装置から伝送されてきた所定の情報に所定の処理を施すことに対する許可に対応する第1のキー-LKを記憶する記憶手段と、所定の情報に対して許可された処理を行う処理手段とを備え、第1のキー-LKは、識別データと、所定の処理を施す情報に対応する第2のキー-SVKに基づいて生成されていることを特徴とする。

【0014】請求項12に記載の情報処理方法は、自分自身に固有の識別データと、他の情報処理装置から伝送されてきた所定の情報に所定の処理を施すことに対する許可に対応する第1のキー-LKを記憶する記憶ステップと、所定の情報に対して許可された処理を行う処理ステップとを備え、第1のキー-LKは、識別データと、所定の処理を施す情報に対応する第2のキー-SVKに基づいて生成されていることを特徴とする。

【0015】請求項13に記載の提供媒体は、自分自身に固有の識別データと、他の情報処理装置から伝送されてきた所定の情報に所定の処理を施すことに対する許可に対応する第1のキー-LKを記憶する記憶ステップと、所定の情報に対して許可された処理を行う処理ステップと

を備え、第1のキー-LKは、識別データと、所定の処理を施す情報に対応する第2のキー-SVKに基づいて生成されているプログラムを提供することを特徴とする。

【0016】請求項14に記載の情報処理装置は、他の情報処理装置に伝送する情報に対応する第1のキー-SVKと、所定の関数を記憶する記憶手段と、他の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信手段と、識別データと第1のキー-SVKに対して関数を適用し、第2のキー-LKを生成する第1の生成手段と、第3のキー-SKを生成する第2の生成手段と、第2のキー-LKを用いて、第3のキー-SKを暗号化し、他の情報処理装置に伝送する暗号化手段とを備えることを特徴とする。

【0017】請求項18に記載の情報処理方法は、他の情報処理装置に伝送する情報に対応する第1のキー-SVKと、所定の関数を記憶する記憶ステップと、他の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信ステップと、識別データと第1のキー-SVKに対して関数を適用し、第2のキー-LKを生成する第1の生成ステップと、第3のキー-SKを生成する第2の生成ステップと、第2のキー-LKを用いて、第3のキー-SKを暗号化し、他の情報処理装置に伝送する暗号化ステップとを備えることを特徴とする。

【0018】請求項19に記載の提供媒体は、他の情報処理装置に伝送する情報に対応する第1のキー-SVKと、所定の関数を記憶する記憶ステップと、他の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信ステップと、識別データと第1のキー-SVKに対して関数を適用し、第2のキー-LKを生成する第1の生成ステップと、第3のキー-SKを生成する第2の生成ステップと、第2のキー-LKを用いて、第3のキー-SKを暗号化し、他の情報処理装置に伝送する暗号化ステップとを備えるプログラムを提供することを特徴とする。

【0019】請求項20に記載の情報処理システムは、第1の情報処理装置は、第2の情報処理装置に伝送する情報に対応する第1のキー-SVKと、所定の関数を記憶する第1の記憶手段と、第2の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信手段と、識別データと第1のキー-SVKに対して関数を適用し、第2のキー-LK1を生成する第1の生成手段と、第3のキー-SK1を生成する第2の生成手段と、第2のキー-LK1を用いて、第3のキー-SK1を暗号化し、第2の情報処理装置に伝送する暗号化手段とを備え、第2の情報処理装置は、自分自身に固有の識別データと、所定の情報に所定の処理を施すことに対する許可に対応する第4のキー-LK2を記憶する第2の記憶手段と、第4のキー-LK2を用いて、第1の情報処理装置から伝送を受けた、暗号化されている第3のキー-SK1を復号する復号手段とを備えることを特徴とする。

【0020】請求項21に記載の情報処理方法は、第1

の情報処理装置は、第2の情報処理装置に伝送する情報に対応する第1のキーSVKと、所定の関数を記憶する第1の記憶ステップと、第2の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信ステップと、識別データと第1のキーSVKに対して関数を適用し、第2のキーLK1を生成する第1の生成ステップと、第3のキーSK1を生成する第2の生成ステップと、第2のキーLK1を用いて、第3のキーSK1を暗号化し、第2の情報処理装置に伝送する暗号化ステップとを備え、第2の情報処理装置は、自分自身に固有の識別データと、所定の情報に所定の処理を施すことに対する許可に対応する第4のキーLK2を記憶する記憶ステップと、第4のキーLK2を用いて、第1の情報処理装置から伝送を受けた、暗号化されている第3のキーSK1を復号する復号ステップとを備えることを特徴とする。

【0021】請求項22に記載の提供媒体は、第1のプログラムは、第2の情報処理装置に伝送する情報に対応する第1のキーSVKと、所定の関数を記憶する第1の記憶ステップと、第2の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信ステップと、識別データと第1のキーSVKに対して関数を適用し、第2のキーLK1を生成する第1の生成ステップと、第3のキーSK1を生成する第2の生成ステップと、第2のキーLK1を用いて、第3のキーSK1を暗号化し、第2の情報処理装置に伝送する暗号化ステップとを備え、第2のプログラムは、自分自身に固有の識別データと、所定の情報に所定の処理を施すことに対する許可に対応する第4のキーLK2を記憶する記憶ステップと、第4のキーLK2を用いて、第1の情報処理装置から伝送を受けた、暗号化されている第3のキーSK1を復号する復号ステップとを備えることを特徴とする。

【0022】請求項23に記載の情報処理装置は、第1のキーLk、第2のキーLk'、および所定の関数Gを記憶する記憶手段と、他の情報処理装置から伝送されてきた所定の情報に対して許可された処理を行う処理手段とを備え、第2のキーLK'は、第1のキーLKと、関数Gの逆関数 G^{-1} に基づいて生成されていることを特徴とする。

【0023】請求項27に記載の情報処理方法は、第1のキーLk、第2のキーLk'、および所定の関数Gを記憶する記憶ステップと、他の情報処理装置から伝送されてきた所定の情報に対して許可された処理を行う処理ステップとを備え、第2のキーLK'は、第1のキーLKと、関数Gの逆関数 G^{-1} に基づいて生成されていることを特徴とする。

【0024】請求項28に記載の提供媒体は、第1のキーLk、第2のキーLk'、および所定の関数Gを記憶する記憶ステップと、他の情報処理装置から伝送されてきた所定の情報に対して許可された処理を行う処理ステップとを備え、第2のキーLK'は、第1のキーLKと、関数G

の逆関数 G^{-1} に基づいて生成されているプログラムを提供することを特徴とする。

【0025】請求項29に記載の情報処理装置は、他の情報処理装置に伝送する情報に対応する第1のキーSVKと、所定の関数を記憶する記憶手段と、他の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信手段と、第2のキーSKを生成する生成手段と、擬似乱数を発生する擬似乱数発生手段と、識別データと第1のキーSVKに対して関数を適用して得られるデータHを、擬似乱数発生手段に適用して得られる疑似乱数 $pRNG(H)$ を用いて、第2のキーSKを暗号化し、他の情報処理装置に伝送する暗号化手段とを備えることを特徴とする。

【0026】請求項30に記載の情報処理方法は、他の情報処理装置に伝送する情報に対応する第1のキーSVKと、所定の関数を記憶する記憶ステップと、他の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信ステップと、第2のキーSKを生成する生成ステップと、擬似乱数を発生する擬似乱数発生ステップと、識別データと第1のキーSVKに対して関数を適用して得られるデータHを、擬似乱数発生ステップに適用して得られる疑似乱数 $pRNG(H)$ を用いて、第2のキーSKを暗号化し、他の情報処理装置に伝送する暗号化ステップとを備えることを特徴とする。

【0027】請求項31に記載の提供媒体は、他の情報処理装置に伝送する情報に対応する第1のキーSVKと、所定の関数を記憶する記憶ステップと、他の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信ステップと、第2のキーSKを生成する生成ステップと、擬似乱数を発生する擬似乱数発生ステップと、識別データと第1のキーSVKに対して関数を適用して得られるデータHを、擬似乱数発生ステップに適用して得られる疑似乱数 $pRNG(H)$ を用いて、第2のキーSKを暗号化し、他の情報処理装置に伝送する暗号化ステップとを備えるプログラムを提供することを特徴とする。

【0028】請求項32に記載の情報処理システムは、第1の情報処理装置は、第2の情報処理装置に伝送する情報に対応する第1のキーSVKと、第1の関数hを記憶する第1の記憶手段と、第2の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信手段と、第2のキーSKを生成する生成手段と、擬似乱数を発生する擬似乱数発生手段と、識別データと第1のキーSVKに対して関数hを適用して得られるデータHを、擬似乱数発生手段に適用して得られる疑似乱数 $pRNG(H)$ を用いて、第2のキーSKを暗号化し、第2の情報処理装置に伝送する暗号化手段とを備え、第2の情報処理装置は、第3のキーLk、第4のキーLk'、および所定の関数Gを記憶する第2の記憶手段と、第1の情報処理装置から伝送されてきた所定の情報に対して許可された処

理を行う処理手段とを備え、第4のキーLK'は、第3のキーLKと、関数Gの逆関数 G^{-1} に基づいて生成されていることを特徴とする。

【0029】請求項33に記載の情報処理方法は、第1の情報処理装置は、第2の情報処理装置に伝送する情報に対応する第1のキーSVKと、所定の関数hを記憶する第1の記憶ステップと、第2の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信ステップと、第2のキーSKを生成する生成ステップと、疑似乱数を発生する疑似乱数発生ステップと、識別データと第1のキーSVKに対して関数hを適用して得られるデータHを、疑似乱数発生ステップに適用して得られる疑似乱数pRNG(H)を用いて、第2のキーSKを暗号化し、第2の情報処理装置に伝送する暗号化ステップとを備え、第2の情報処理装置は、第3のキーLk、第4のキーLk'、および所定の関数Gを記憶する第2の記憶ステップと、第1の情報処理装置から伝送されてきた所定の情報に対して許可された処理を行う処理ステップとを備え、第4のキーLK'は、第3のキーLKと、関数Gの逆関数 G^{-1} に基づいて生成されていることを特徴とする。

【0030】請求項34に記載の提供媒体は、第1のプログラムは、第2の情報処理装置に伝送する情報に対応する第1のキーSVKと、所定の関数hを記憶する第1の記憶ステップと、第2の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信ステップと、第2のキーSKを生成する生成ステップと、疑似乱数を発生する疑似乱数発生ステップと、識別データと第1のキーSVKに対して関数hを適用して得られるデータHを、疑似乱数発生ステップに適用して得られる疑似乱数pRNG(H)を用いて、第2のキーSKを暗号化し、第2の情報処理装置に伝送する暗号化ステップとを備え、第2のプログラムは、第3のキーLk、第4のキーLk'、および所定の関数Gを記憶する第2の記憶ステップと、第1の情報処理装置から伝送されてきた所定の情報に対して許可された処理を行う処理ステップとを備え、第4のキーLK'は、第3のキーLKと、関数Gの逆関数 G^{-1} に基づいて生成されていることを特徴とする。

【0031】請求項1に記載の情報処理装置、請求項12に記載の情報処理方法、および請求項13に記載の提供媒体においては、第1のキーLKが、識別データと、所定の処理を施す情報に対応する第2のキーSVKに基づいて生成されている。

【0032】請求項14に記載の情報処理装置、請求項18に記載の情報処理方法、および請求項19に記載の提供媒体においては、第1のキーSVKと、所定の関数が記憶されている。他の情報処理装置から、伝送されてきた識別データと第1のキーSVKに対して関数を適用して、第2のキーLKが生成される。さらに、第3のキーSKが生成され、第2のキーLKを用いて、第3のキーSKが暗号化され、他の情報処理装置に伝送される。

【0033】請求項20に記載の情報処理システム、請求項21に記載の情報処理方法、および請求項22に記載の提供媒体においては、第1の情報処理装置が、第2の情報処理装置に伝送する情報に対応する第1のキーSVKと、所定の関数を記憶し、第2の情報処理装置から、伝送されてきた、識別データと第1のキーSVKに対して関数を適用して、第2のキーLK1を生成する。また、第3のキーSK1を生成し、これを第2のキーLK1を用いて暗号化し、第2の情報処理装置に伝送する。第2の情報処理装置においては、自分自身に固有の識別データと、所定の情報に所定の処理を施すことに対する許可に対応する第4のキーLK2が記憶されている。第4のキーLK2を用いて、第1の情報処理装置から伝送を受けた、暗号化されている第3のキーSK1が復号される。

【0034】請求項23に記載の情報処理装置、請求項27に記載の情報処理方法、および請求項28に記載の提供媒体においては、第1のキーLk、第2のキーLk'、および所定の関数Gが記憶されており、第2のキーLK'は、第1のキーLKと、関数Gの逆関数 G^{-1} に基づいて生成される。

【0035】請求項29に記載の情報処理装置、請求項30に記載の情報処理方法、および請求項31に記載の提供媒体においては、他の情報処理装置から伝送されてきた識別データと、第1のキーSVKに対して関数を適用して得られるデータHから発生された疑似乱数pRNG(H)を用いて、第2のキーSKが暗号化され、他の情報処理装置に伝送される。

【0036】請求項32に記載の情報処理システム、請求項33に記載の情報処理方法、および請求項34に記載の提供媒体においては、第1の情報処理装置において、第2の情報処理装置の識別データと、第1のキーSVKに対して関数hを適用して得られるデータHから発生された疑似乱数pRNG(H)を用いて、第2のキーSKが暗号化され、第2の情報処理装置に伝送される。第2の情報処理装置においては、第3のキーLk、第4のキーLk'、および所定の関数Gが記憶され、第4のキーLK'は、第3のキーLKと、関数Gの逆関数 G^{-1} に基づいて生成される。

【0037】

【発明の実施の形態】以下に本発明の実施の形態を説明するが、特許請求の範囲に記載の発明の各手段と以下の実施の形態との対応関係を明らかにするために、各手段の後の括弧内に、対応する実施の形態（但し一例）を付加して本発明の特徴を記述すると、次のようになる。但し勿論この記載は、各手段を記載したものに限定的であることを意味するものではない。

【0038】請求項1に記載の情報処理装置は、自分自身に固有の識別データと、他の情報処理装置から伝送されてきた所定の情報に所定の処理を施すことに対する許可に対応する第1のキーLK（例えば、license_key）を

記憶する記憶手段（例えば、図2のEEPROM50）と、所定の情報に対して許可された処理を行う処理手段（例えば、図2のCPU41）とを備え、第1のキーLKは、識別データ（例えば、ID）と、所定の処理を施す情報に対応する第2のキーSVK（例えば、service_key）に基づいて生成されていることを特徴とする。

【0039】請求項2に記載の情報処理装置は、第1のキーLKを用いて、他の情報処理装置から伝送されてきた暗号化されている第3のキーSK（例えば、暗号鍵sk）を復号するキー復号手段（例えば、図4のステップS10）をさらに備えることを特徴とする。

【0040】請求項3に記載の情報処理装置は、第3のキーSKを用いて、他の情報処理装置から伝送されてくる暗号化されている情報を復号する情報復号手段（例えば、図2のCPU41）をさらに備えることを特徴とする。

【0041】請求項4に記載の情報処理装置は、第3のキーSKは、1つのセッションにおいて不変の第4のキーSS（例えば、初期値キーSs）と、セッション内において変更される第5のキーSi（例えば、攪乱キーSi）とにより構成されていることを特徴とする。

【0042】請求項5に記載の情報処理装置は、伝送されてきた情報を復号する乱数を発生する乱数発生手段（例えば、図28の乱数発生器914）と、第4のキーSS、または乱数発生手段により発生された乱数で復号された情報を用いて、乱数発生手段が乱数を発生するときの初期値を演算する演算手段（例えば、図28の演算回路913）とをさらに備えることを特徴とする。

【0043】請求項9に記載の情報処理装置は、他の情報処理装置から識別データの伝送の要求があったとき、識別データを他の情報処理装置に伝送する伝送手段（例えば、図4のステップS3）をさらに備えることを特徴とする。

【0044】請求項10に記載の情報処理装置は、第1のキーLKを、所定の関数を用いて更新する更新手段（例えば、図26のステップS167）をさらに備えることを特徴とする。

【0045】請求項11に記載の情報処理装置は、他の情報処理装置から伝送されてきた、暗号化されている情報を第3のキーSKを用いて復号した結果に対応して、第1のキーLKを更新する更新手段（例えば、図27のステップS170）をさらに備えることを特徴とする。

【0046】請求項12に記載の情報処理方法は、自分自身に固有の識別データ（例えば、ID）と、他の情報処理装置から伝送されてきた所定の情報に所定の処理を施すことに対する許可に対応する第1のキーLK（例えば、license_key）を記憶する記憶ステップ（例えば、図4のEEPROM50）と、所定の情報に対して許可された処理を行う処理ステップとを備え、第1のキーLKは、識別データと、所定の処理を施す情報に対応する第2のキーSV

K（例えば、service_key）に基づいて生成されていることを特徴とする。

【0047】請求項14に記載の情報処理装置は、他の情報処理装置に伝送する情報に対応する第1のキーSVK（例えば、service_key）と、所定の関数（例えば、hash関数）を記憶する記憶手段（例えば、図2のEEPROM27）と、他の情報処理装置から、それに割り当てられている識別データの伝送を受け、受信する受信手段（例えば、図4のステップS4）と、識別データと第1のキーSVKに対して関数を適用し、第2のキーLK（例えば、鍵lk）を生成する第1の生成手段（例えば、図4のステップS5）と、第3のキーSK（例えば、暗号鍵sk）を生成する第2の生成手段（例えば、図4のステップS6）と、第2のキーLKを用いて、第3のキーSKを暗号化し、他の情報処理装置に伝送する暗号化手段（例えば、図4のステップS7、S8）とを備えることを特徴とする。

【0048】請求項18に記載の情報処理方法は、他の情報処理装置に伝送する情報に対応する第1のキーSVK（例えば、service_key）と、所定の関数（例えば、hash関数）を記憶する記憶ステップ（例えば、図2のEEPROM27）と、他の情報処理装置から、それに割り当てられている識別データの（例えば、ID）伝送を受け、受信する受信ステップ（例えば、図4のステップS4）と、識別データと第1のキーSVKに対して関数を適用し、第2のキーLK（例えば、鍵lk）を生成する第1の生成ステップ（例えば、図4のステップS5）と、第3のキーSK（例えば、暗号鍵sk）を生成する第2の生成ステップ（例えば、図4のステップS6）と、第2のキーLKを用いて、第3のキーSKを暗号化し、他の情報処理装置に伝送する暗号化ステップ（例えば、図4のステップS7、S8）とを備えることを特徴とする。

【0049】請求項20に記載の情報処理システムは、第1の情報処理装置（例えば、図4のソース）は、第2の情報処理装置（例えば、図4のシンク）に伝送する情報に対応する第1のキーSVK（例えば、service_key）と、所定の関数（例えば、hash関数）を記憶する第1の記憶手段（例えば、図2のEEPROM27）と、第2の情報処理装置から、それに割り当てられている識別データ（例えば、ID）の伝送を受け、受信する受信手段（例えば、図4のステップS4）と、識別データと第1のキーSVKに対して関数を適用し、第2のキーLK1（例えば、鍵lk）を生成する第1の生成手段（例えば、図4のステップS5）と、第3のキーSK1（例えば、暗号鍵sk）を生成する第2の生成手段（例えば、図4のステップS6）と、第2のキーLK1を用いて、第3のキーSK1を暗号化し、第2の情報処理装置に伝送する暗号化手段（例えば、図4のステップS7、S8）とを備え、第2の情報処理装置は、自分自身に固有の識別データと、所定の情報に所定の処理を施すことに対する許可に対応する第4のキーLK2（例えば、license_key）を記憶する第2の記

憶手段（例えば、図2のEEPROM 50）と、第4のキーLK2を用いて、第1の情報処理装置から伝送を受けた、暗号化されている第3のキーSK1を復号する復号手段（例えば、図4のステップS10）とを備えることを特徴とする。

【0050】請求項21に記載の情報処理方法は、第1の情報処理装置（例えば、図4のソース）は、第2の情報処理装置（例えば、図4のシンク）に伝送する情報に対応する第1のキーSVK（例えば、service_key）と、所定の関数（例えば、hash関数）を記憶する第1の記憶ステップ（例えば、図2のEEPROM 27）と、第2の情報処理装置から、それに割り当てられている識別データ（例えば、ID）の伝送を受け、受信する受信ステップ（例えば、図4のステップS4）と、識別データと第1のキーSVKに対して関数を適用し、第2のキーLK1（例えば、鍵lk）を生成する第1の生成ステップ（例えば、図4のステップS5）と、第3のキーSK1（例えば、暗号鍵sk）を生成する第2の生成ステップ（例えば、図4のステップS6）と、第2のキーLK1を用いて、第3のキーSK1を暗号化し、第2の情報処理装置に伝送する暗号化ステップ（例えば、図4のステップS7）とを備え、第2の情報処理装置は、自分自身に固有の識別データと、所定の情報に所定の処理を施すことに対する許可に対応する第4のキーLK2（例えば、license_key）を記憶する記憶ステップ（例えば、図2のEEPROM 50）と、第4のキーLK2を用いて、第1の情報処理装置から伝送を受けた、暗号化されている第3のキーSK1を復号する復号ステップ（例えば、図4のステップS10）とを備えることを特徴とする。

【0051】請求項23に記載の情報処理装置は、第1のキーLk（例えば、図9のLK）、第2のキーLk'（例えば、図9のLK'）、および所定の関数G（例えば、図9の関数G）を記憶する記憶手段（例えば、図9のEEPROM 50）と、他の情報処理装置から伝送されてきた所定の情報に対して許可された処理を行う処理手段（例えば、図2のCPU 41）とを備え、第2のキーLk'は、第1のキーLkと、関数Gの逆関数 G^{-1} に基づいて生成されていることを特徴とする。

【0052】請求項24に記載の情報処理装置は、擬似乱数を発生する擬似乱数発生手段（例えば、図9のpRNG）をさらに備え、記憶手段は、自分自身に固有の識別データをさらに記憶することを特徴とする。

【0053】請求項26に記載の情報処理装置は、他の情報処理装置から伝送されてきた、擬似乱数pRNG(H)を用いて暗号化されている第4のキーSKを、第2のキーLK'を関数Gに適用して得られるデータG(LK')と、擬似乱数pRNG(LK)を用いて復号するキー復号手段（例えば、図9のステップS110）をさらに備えることを特徴とする。

【0054】請求項27に記載の情報処理方法は、第1

のキーLk（例えば、図9のLK）、第2のキーLk'（例えば、図9のLK'）、および所定の関数G（例えば、図9の関数G）を記憶する記憶ステップ（例えば、図9のEEPROM 50）と、他の情報処理装置から伝送されてきた所定の情報に対して許可された処理を行う処理ステップ（例えば、図2のCPU 41）とを備え、第2のキーLk'は、第1のキーLkと、関数Gの逆関数 G^{-1} に基づいて生成されていることを特徴とする。

【0055】請求項29に記載の情報処理装置は、他の情報処理装置に伝送する情報に対応する第1のキーSVK（例えば、図9のservice_key）と、所定の関数（例えば、hash関数）を記憶する記憶手段（例えば、図9のEEPROM 27）と、他の情報処理装置から、それに割り当てられている識別データ（例えば、ID）の伝送を受け、受信する受信手段（例えば、図9のステップS104）と、第2のキーSK（例えば、図9のsk）を生成する生成手段（例えば、図9のステップS106）と、擬似乱数を発生する擬似乱数発生手段（例えば、図9のpRNG）と、識別データと第1のキーSVKに対して関数を適用して得られるデータHを、擬似乱数発生手段に適用して得られる疑似乱数pRNG(H)を用いて、第2のキーSKを暗号化し、他の情報処理装置に伝送する暗号化手段（例えば、図9のステップS107、108）とを備えることを特徴とする。

【0056】請求項30に記載の情報処理方法は、他の情報処理装置に伝送する情報に対応する第1のキーSVK（例えば、図9のservice_key）と、所定の関数（例えば、hash関数）を記憶する記憶ステップ（例えば、図9のEEPROM 27）と、他の情報処理装置から、それに割り当てられている識別データ（例えば、ID）の伝送を受け、受信する受信ステップ（例えば、図9のステップS104）と、第2のキーSK（例えば、図9のsk）を生成する生成ステップ（例えば、図9のステップS106）と、擬似乱数を発生する擬似乱数発生ステップ（例えば、図9のpRNG）と、識別データと第1のキーSVKに対して関数を適用して得られるデータHを、擬似乱数発生ステップに適用して得られる疑似乱数pRNG(H)を用いて、第2のキーSKを暗号化し、他の情報処理装置に伝送する暗号化ステップ（例えば、図9のステップS107、108）とを備えることを特徴とする。

【0057】請求項32に記載の情報処理システムは、第1の情報処理装置（例えば、図9のソース）が、第2の情報処理装置（例えば、図9のシンク）に伝送する情報に対応する第1のキーSVK（例えば、図9のservice_key）と、第1の関数h（例えば、hash関数）を記憶する第1の記憶手段（例えば、図9のEEPROM 27）と、第2の情報処理装置から、それに割り当てられている識別データ（例えば、ID）の伝送を受け、受信する受信手段（例えば、図9のステップS104）と、第2のキーSK（例えば、図9のsk）を生成する生成手段（例えば、図

9のステップS106)と、擬似乱数を発生する擬似乱数発生手段(例えば、図9のpRNG)と、識別データと第1のキーSVKに対して関数hを適用して得られるデータHを、擬似乱数発生手段に適用して得られる疑似乱数pRNG(H)を用いて、第2のキーSKを暗号化し、第2の情報処理装置に伝送する暗号化手段(例えば、図9のステップS107、108)とを備え、第2の情報処理装置が、第3のキーLk(例えば、図9のLK)、第4のキーLk'(例えば、図9のLk')、および所定の関数G(例えば、図9の関数G)を記憶する第2の記憶手段(例えば、図9のEEPROM50)と、第1の情報処理装置から伝送されてきた所定の情報に対して許可された処理を行う処理手段(例えば、図2のCPU41)とを備え、第4のキーLk'は、第3のキーLKと、関数Gの逆関数 G^{-1} に基づいて生成されていることを特徴とする。

【0058】請求項33に記載の情報処理方法は、第1の情報処理装置(例えば、図9のソース)が、第2の情報処理装置(例えば、図9のシンク)に伝送する情報に対応する第1のキーSVK(例えば、図9のservice_key)と、所定の関数h(例えば、hash関数)を記憶する第1の記憶ステップ(例えば、図9のEEPROM27)と、第2の情報処理装置から、それに割り当てられている識別データ(例えば、ID)の伝送を受け、受信する受信ステップ(例えば、図9のステップS104)と、第2のキーSK(例えば、図9のsk)を生成する生成ステップ(例えば、図9のステップS106)と、擬似乱数を発生する擬似乱数発生ステップ(例えば、図9のpRNG)と、識別データと第1のキーSVKに対して関数hを適用して得られるデータHを、擬似乱数発生ステップに適用して得られる疑似乱数pRNG(H)を用いて、第2のキーSKを暗号化し、第2の情報処理装置に伝送する暗号化ステップ(例えば、図9のステップS107、108)とを備え、第2の情報処理装置が、第3のキーLk(例えば、図9のLK)、第4のキーLk'(例えば、図9のLk')、および所定の関数G(例えば、図9の関数G)を記憶する第2の記憶ステップ(例えば、図9のEEPROM50)と、第1の情報処理装置から伝送されてきた所定の情報に対して許可された処理を行う処理ステップ(例えば、図2のCPU41)とを備え、第4のキーLk'は、第3のキーLKと、関数Gの逆関数 G^{-1} に基づいて生成されていることを特徴とする。

【0059】図1は、本発明を適用した情報処理システムの構成例を表している。この構成例においては、IEEE1394シリアルバス11を介してDVDプレーヤ1、パーソナルコンピュータ2、光磁気ディスク装置3、データ放送受信装置4、モニタ5、テレビジョン受像機6が相互に接続されている。

【0060】図2は、この内のDVDプレーヤ1、パーソナルコンピュータ2、および光磁気ディスク装置3の内部のより詳細な構成例を表している。DVDプレーヤ1

は、1394インタフェース26を介して、1394バス11に接続されている。CPU21は、ROM22に記憶されているプログラムに従って各種の処理を実行し、RAM23は、CPU21が各種の処理を実行する上において必要なデータやプログラムなどを適宜記憶する。操作部24は、ボタン、スイッチ、リモートコントローラなどにより構成され、ユーザにより操作されたとき、その操作に対応する信号を出力する。ドライブ25は、図示せぬDVD(ディスク)を駆動し、そこに記録されているデータを再生するようになされている。EEPROM27は、装置の電源オフ後も記憶する必要がある情報(この実施の形態の場合、鍵情報)を記憶するようになされている。内部バス28は、これらの各部を相互に接続している。

【0061】光磁気ディスク装置3は、CPU31乃至内部バス38を有している。これらは、上述したDVDプレーヤ1におけるCPU21乃至内部バス28と同様の機能を有するものであり、その説明は省略する。ただし、ドライブ35は、図示せぬ光磁気ディスクを駆動し、そこにデータを記録または再生するようになされている。

【0062】パーソナルコンピュータ2は、1394インタフェース49を介して1394バス11に接続されている。CPU41は、ROM42に記憶されているプログラムに従って各種の処理を実行する。RAM43には、CPU41が各種の処理を実行する上において必要なデータやプログラムなどが適宜記憶される。入出力インタフェース44には、キーボード45とマウス46が接続されており、それらから入力された信号をCPU41に出力するようになされている。また、入出力インタフェース44には、ハードディスク(HDD)47が接続されており、そこにデータ、プログラムなどを記録再生することができるようになされている。入出力インタフェース44にはまた、拡張ボード48を適宜装着し、必要な機能を付加することができるようになされている。EEPROM50には、電源オフ後も保持する必要がある情報(この実施の形態の場合、各種の鍵情報)が記憶されるようになされている。例えば、PCI(Peripheral Component Interconnect)、ローカルバスなどにより構成される内部バス51は、これらの各部を相互に接続するようになされている。

【0063】なお、この内部バス51は、ユーザに対して解放されており、ユーザは、拡張ボード48に所定のボードを適宜接続したり、所定のソフトウェアプログラムを作成して、CPU41にインストールすることで、内部バス51により伝送されるデータを適宜受信することができるようになされている。

【0064】これに対して、DVDプレーヤ1や光磁気ディスク装置3などのコンシューマエレクトロニクス(CE)装置においては、内部バス28や内部バス38は、ユーザに解放されておらず、特殊な改造などを行わない限り、そこに伝送されるデータを取得することができな

いようになされている。

【0065】次に、所定のソースとシンクとの間で行われる認証の処理について説明する。この認証の処理は、図3に示すように、ソースとしての、例えばDVDプレーヤ1のROM22に予め記憶されているソフトウェアプログラムの1つとしてのファームウェア20と、シンクとしての、例えばパーソナルコンピュータ2のROM42に記憶されており、CPU41が処理するソフトウェアプログラムの1つとしてのライセンスマネージャ62との間において行われる。

【0066】図4は、ソース（DVDプレーヤ1）と、シンク（パーソナルコンピュータ2）の間において行われる認証の手順を示している。DVDプレーヤ1のEEPROM27には、サービスキー（service_key）と関数（hash）が予め記憶されている。これらはいずれも著作権者から、このDVDプレーヤ1のユーザに与えられたものであり、各ユーザは、EEPROM27に、これを秘密裡に保管しておくものである。

【0067】サービスキーは、著作権者が提供する情報毎に与えられるものであり、この1394バス11で構成されるシステムにおいて、共通のものである。なお、本明細書において、システムとは、複数の装置で構成される全体的な装置を示すものとする。

【0068】hash関数は、任意長の入力に対して、64ビットまたは128ビットなどの固定長のデータを出力する関数であり、 $y (=hash(x))$ を与えられたとき、 x を求めることが困難であり、かつ、 $hash(x1) = hash(x2)$ となる $x1$ と、 $x2$ の組を求めることも困難となる関数である。1方向hash関数の代表的なものとして、MD5やSHAなどが知られている。この1方向hash関数については、BruceSchneier著の「Applied Cryptography(Second Edition),Wiley」に詳しく解説されている。

【0069】一方、シンクとしての例えばパーソナルコンピュータ2は、著作権者から与えられた、自分自身に固有の識別番号（ID）とライセンスキー（license_key）をEEPROM50に秘密裡に保持している。このライセンスキーは、 n ビットのIDと m ビットのサービスキーを連結して得た $n+m$ ビットのデータ（ID || service_key）に対して、hash関数を適用して得られる値である。すなわち、ライセンスキーは次式で表される。

$licence_key = hash(ID || service_key)$

【0070】IDとしては、例えば1394バス11の規格に定められているnode_unique_IDを用いることができる。このnode_unique_IDは、図5に示すように、8バイト（64ビット）で構成され、最初の3バイトは、IEEEで管理され、電子機器の各メーカーにIEEEから付与される。また、下位5バイトは、各メーカーが、自分自身がユーザに提供する各装置に対して付与することができるものである。各メーカーは、例えば下位5バイトに対し

てシリアルに、1台に1個の番号を割り当てるようにし、5バイト分を全部使用した場合には、上位3バイトがさらに別の番号となっているnode_unique_IDの付与を受け、そして、その下位5バイトについて1台に1個の番号を割り当てるようにする。従って、このnode_unique_IDは、メーカーに拘らず、1台毎に異なるものとなり、各装置に固有のものとなる。

【0071】ステップS1において、DVDプレーヤ1のファームウェア20は、1394インタフェース26を制御し、1394バス11を介してパーソナルコンピュータ2に対してIDを要求する。パーソナルコンピュータ2のライセンスマネージャ62は、ステップS2において、このIDの要求を受信する。すなわち、1394インタフェース49は、1394バス11を介してDVDプレーヤ1から伝送されてきたID要求の信号を受信すると、これをCPU41に出力する。CPU41のライセンスマネージャ62は、このID要求を受けたとき、ステップS3においてEEPROM50に記憶されているIDを読み出し、これを1394インタフェース49を介して1394バス11からDVDプレーヤ1に伝送する。

【0072】DVDプレーヤ1においては、ステップS4で1394インタフェース26が、このIDを受け取ると、このIDがCPU21で動作しているファームウェア20に供給される。

【0073】ファームウェア20は、ステップS5において、パーソナルコンピュータ2から伝送を受けたIDと、EEPROM27に記憶されているサービスキーを連結して、連結データ（ID || service_key）を生成し、このデータに対して、次式に示すようにhash関数を適用して、キーlkを生成する。

$lk = hash(ID || service_key)$

【0074】次に、ステップS6において、ファームウェア20は、暗号鍵skを生成する。この暗号鍵skの詳細については後述するが、この暗号鍵skは、セッションキーとしてDVDプレーヤ1とパーソナルコンピュータ2のそれぞれにおいて利用される。

【0075】次に、ステップS7において、ファームウェア20は、ステップS5で生成した鍵lkを鍵として、ステップS6で生成した暗号鍵skを暗号化して、暗号化データ（暗号化鍵）eを得る。すなわち、次式を演算する。

$e = Enc(lk, sk)$

【0076】なお、Enc(A, B)は、共通鍵暗号方式で、鍵Aを用いて、データBを暗号化することを意味する。

【0077】次に、ステップS8で、ファームウェア20は、ステップS7で生成した暗号化データeをパーソナルコンピュータ2に伝送する。すなわち、この暗号化データeは、DVDプレーヤ1の1394インタフェース26から1394バス11を介してパーソナルコンピュ

ータ2に伝送される。パーソナルコンピュータ2においては、ステップS9で、この暗号化データeを1394インタフェース49を介して受信する。ライセンスマネージャ62は、このようにして受信した暗号化データeをEEPROM50に記憶されているライセンスキーを鍵として、次式に示すように復号し、復号鍵sk'を生成する。

$$sk' = \text{Dec}(\text{license_key}, e)$$

【0078】なお、ここで、Dec(A, B)は、共通鍵暗号方式で鍵Aを用いて、データBを復号することを意味する。

【0079】なお、この共通鍵暗号方式における暗号化のアルゴリズムとしては、DESが知られている。共通鍵暗号化方式についても、上述した、Applied Cryptography(Second Edition)に詳しく解説されている。

【0080】DVDプレーヤ1において、ステップS5で生成するキーlkは、パーソナルコンピュータ2のEEPROM50に記憶されている(license_key)と同一の値となる。すなわち、次式が成立する。

$$lk = \text{license_key}$$

【0081】従って、パーソナルコンピュータ2において、ステップS10で復号して得たキーsk'は、DVDプレーヤ1において、ステップS6で生成した暗号鍵skと同一の値となる。すなわち、次式が成立する。

$$sk' = sk$$

【0082】このように、DVDプレーヤ1(ソース)とパーソナルコンピュータ2(シンク)の両方において、同一の鍵sk, sk'を共有することができる。そこで、この鍵skをそのまま暗号鍵として用いるか、あるいは、これを基にして、それぞれが疑似乱数を作り出し、それを暗号鍵として用いることができる。

【0083】ライセンスキーは、上述したように、各装置に固有のIDと、提供する情報に対応するサービスキーに基づいて生成されているので、他の装置がskまたはsk'を生成することはできない。また、著作権者から認められていない装置は、ライセンスキーを有していないので、skあるいはsk'を生成することができない。従って、その後DVDプレーヤ1が暗号鍵skを用いて再生データを暗号化してパーソナルコンピュータ2に伝送した場合、パーソナルコンピュータ2が適正にライセンスキーを得たものである場合には、暗号鍵sk'を有しているので、DVDプレーヤ1より伝送されてきた、暗号化されている再生データを復号することができる。しかしながら、パーソナルコンピュータ2が適正なものでない場合、暗号鍵sk'を有していないので、伝送されてきた暗号化されている再生データを復号することができない。換言すれば、適正な装置だけが共通の暗号鍵sk, sk'を生成することができるので、結果的に、認証が行われることになる。

【0084】仮に1台のパーソナルコンピュータ2のライセンスキーが盗まれたとしても、IDが1台1台異なる

ので、そのライセンスキーを用いて、他の装置がDVDプレーヤ1から伝送されてきた暗号化されているデータを復号することはできない。従って、安全性が向上する。

【0085】ところで、何らかの理由により、不正なユーザが、暗号化データeと暗号鍵skを両方とも知ってしまったような場合のことを考える。この場合、eは、平文skを、鍵lkで暗号化した暗号文であるので、暗号アルゴリズムが公開されている場合、不正ユーザは、鍵lkを総当たりで試すことにより、正しい鍵lkを得る可能性がある。

【0086】不正ユーザによるこの種の攻撃を、より困難にするためには、暗号アルゴリズムの一部または全部を一般に公開せずに秘密にしておくことができる。

【0087】または同様に、license_keyから、service_keyを総当たりで調べる攻撃を、より困難にするために、hash関数の一部または全文を一般に公開せずに秘密にしておくようにすることもできる。

【0088】図6は、ソース(DVDプレーヤ1)に対して、パーソナルコンピュータ2だけでなく、光磁気ディスク装置3もシンクとして機能する場合の処理例を表している。

【0089】この場合、シンク1としてのパーソナルコンピュータ2のEEPROM50には、IDとしてID1が、また、ライセンスキーとしてlicense_key1が記憶されており、シンク2としての光磁気ディスク装置3においては、EEPROM37に、IDとしてID2が、また、ライセンスキーとしてlicense_key2が記憶されている。

【0090】DVDプレーヤ1(ソース)とパーソナルコンピュータ2(シンク1)の間において行われるステップS11乃至ステップS20の処理は、図4におけるステップS1乃至ステップS10の処理と実質的に同様の処理であるので、その説明は省略する。

【0091】すなわち、上述したようにして、DVDプレーヤ1は、パーソナルコンピュータ2に対して認証処理を行う。そして次に、ステップS21において、DVDプレーヤ1は、光磁気ディスク装置3に対して、IDを要求する。光磁気ディスク装置3においては、ステップS22で1394インタフェース36を介して、このID要求信号が受信されると、そのファームウェア30(図10)は、ステップS23でEEPROM37に記憶されているID(ID2)を読み出し、これを1394インタフェース36から、1394バス11を介してDVDプレーヤ1に伝送する。DVDプレーヤ1のファームウェア20は、ステップS24で、1394インタフェース26を介して、このID2を受け取ると、ステップS25で、次式から鍵lk2を生成する。

$$lk2 = \text{hash}(ID2 \parallel \text{service_key})$$

【0092】さらに、ファームウェア20は、ステップS26で次式を演算し、ステップS16で生成した鍵skを、ステップS25で生成した鍵lk2を用いて暗号化

し、暗号化したデータ e_2 を生成する。

$e_2 = \text{Enc}(lk_2, sk)$

【0093】そして、ステップS27で、ファームウェア20は、この暗号化データ e_2 を1394インタフェース26から1394バス11を介して光磁気ディスク装置3に伝送する。

【0094】光磁気ディスク装置3においては、ステップS28で1394インタフェース36を介して、この暗号化データ e_2 を受信し、ステップS29で次式を演算して、暗号鍵 sk_2' を生成する。

$sk_2' = \text{Dec}(\text{license_key}_2, e_2)$

【0095】以上のようにして、パーソナルコンピュータ2と光磁気ディスク装置3のそれぞれにおいて、暗号鍵 sk_1' 、 sk_2' が得られたことになる。これらの値は、DVDプレーヤ1における暗号鍵 sk と同一の値となっている。

【0096】図6の処理例においては、DVDプレーヤ1が、パーソナルコンピュータ2と、光磁気ディスク装置3に対して、それぞれ個別にIDを要求し、処理するようにしているのであるが、同報通信によりIDを要求することができる場合は、図7に示すような処理を行うことができる。

【0097】すなわち、図7の処理例においては、ステップS41で、ソースとしてのDVDプレーヤ1が、全てのシンク（この例の場合、パーソナルコンピュータ2と光磁気ディスク装置3）に対して同報通信でIDを要求する。パーソナルコンピュータ2と光磁気ディスク装置3は、それぞれステップS42とステップS43で、このID転送要求の信号を受け取ると、それぞれステップS44またはステップS45で、EEPROM50またはEEPROM37に記憶されているID1またはID2を読み出し、これをDVDプレーヤ1に転送する。DVDプレーヤ1は、ステップS46とステップS47で、これらのIDをそれぞれ受信する。

【0098】DVDプレーヤ1においては、さらにステップS48で、次式から暗号鍵 lk_1 を生成する。

$lk_1 = \text{hash}(ID_1 || \text{service_key})$

【0099】さらに、ステップS49において、次式から暗号鍵 lk_2 が生成される。

$lk_2 = \text{hash}(ID_2 || \text{service_key})$

【0100】DVDプレーヤ1においては、さらにステップS50で、暗号鍵 sk が生成され、ステップS51で、次式で示すように、暗号鍵 sk が、鍵 lk_1 を鍵として暗号化される。

$e_1 = \text{Enc}(lk_1, sk)$

【0101】さらに、ステップS52においては、暗号鍵 sk が、鍵 lk_2 を鍵として、次式に従って暗号化される。

$e_2 = \text{Enc}(lk_2, sk)$

【0102】さらに、ステップS53においては、ID

1、 e_1 、ID2、 e_2 が、それぞれ次式で示すように連結されて、暗号化データ e が生成される。

$e = ID_1 || e_1 || ID_2 || e_2$

【0103】DVDプレーヤ1においては、さらにステップS54で、以上のようにして生成された暗号化データ e が同報通信で、パーソナルコンピュータ2と光磁気ディスク装置3に伝送される。

【0104】パーソナルコンピュータ2と光磁気ディスク装置3においては、それぞれステップS55またはステップS56で、これらの暗号化データ e が受信される。そして、パーソナルコンピュータ2と光磁気ディスク装置3においては、それぞれステップS57またはステップS58において、次式で示す演算が行われ、暗号鍵 sk_1' 、 sk_2' が生成される。

$sk_1' = \text{Dec}(\text{license_key}_1, e_1)$

$sk_2' = \text{Dec}(\text{license_key}_2, e_2)$

【0105】図8は、1つのシンクが複数のサービスを受けること（複数の種類の情報の復号）ができるようになされている場合の処理例を表している。すなわち、この場合においては、例えば、シンクとしてのパーソナルコンピュータ2は、複数のライセンスキー（ license_key_1 、 license_key_2 、 license_key_3 など）をEEPROM50に記憶している。ソースとしてのDVDプレーヤ1は、そのEEPROM27に複数のサービスキー（ service_key_1 、 service_key_2 、 service_key_3 など）を記憶している。この場合、DVDプレーヤ1は、ステップS81でシンクとしてのパーソナルコンピュータ2に対してIDを要求するとき、DVDプレーヤ1が、これから転送しようとする情報（サービス）を識別する service_ID を転送する。パーソナルコンピュータ2においては、ステップS82で、これを受信したとき、EEPROM50に記憶されている複数のライセンスキーの中から、この service_ID に対応するものを選択し、これを用いて、ステップS90で復号処理を行う。その他の動作は、図4における場合と同様である。

【0106】図9は、さらに他の処理例を表している。この例においては、ソースとしてのDVDプレーヤ1が、そのEEPROM27に、 service_key 、 hash 関数、および疑似乱数発生関数 pRNG を記憶している。これらは、著作権者から与えられたものであり、秘密裡に保管される。また、シンクとしてのパーソナルコンピュータ2のEEPROM50には、著作権者から与えられたID、LK、LK'、関数G、および疑似乱数発生関数 pRNG を有している。

【0107】LKは、著作権者が作成したユニークな乱数であり、LK'は、次式を満足するように生成されている。

$LK' = G^{-1}(R)$

$R = \text{pRNG}(H) (+) \text{pRNG}(LK)$

$H = \text{hash}(ID || \text{service_key})$

【0108】なお、 G^{-1} （ \wedge はべき乗を意味する）

は、Gの逆関数を意味する。 G^{-1} は、所定の規則を知っていれば、簡単に計算することができるが、知らない場合には、計算することが難しいような特徴を有している。このような関数としては、公開鍵暗号に用いられている関数を利用することができる。

【0109】また、疑似乱数発生関数は、ハードウェアとして設けるようにすることも可能である。

【0110】DVDプレーヤ1のファームウェア20は、最初にステップS101において、パーソナルコンピュータ2のライセンスマネージャ62に対してIDを要求する。パーソナルコンピュータ2のライセンスマネージャ62は、ステップS102でID要求信号を受け取ると、EEPROM50に記憶されているIDを読み出し、ステップS103で、これをDVDプレーヤ1に伝送する。DVDプレーヤ1のファームウェア20は、ステップS104でこのIDを受け取ると、ステップS105で次式を演算する。
 $H = \text{hash}(\text{ID} \parallel \text{service_key})$

【0111】さらに、ファームウェア20は、ステップS106で鍵skを生成し、ステップS107で次式を演算する。

$$e = \text{sk} (+) \text{pRNG}(H)$$

【0112】なお、 $A (+) B$ は、AとBの排他的論理

$$\begin{aligned} \text{sk}' &= e (+) G(LK') (+) \text{pRNG}(LK) \\ &= \text{sk} (+) \text{pRNG}(H) (+) R (+) \text{pRNG}(LK) \\ &= \text{sk} (+) \text{pRNG}(H) (+) \text{pRNG}(H) (+) \text{pRNG}(LK) (+) \\ &\quad \text{pRNG}(LK) \\ &= \text{sk} \end{aligned}$$

【0118】このようにして、ソースとしてのDVDプレーヤ1とシンクとしてのパーソナルコンピュータ2は、同一の鍵sk, sk'を共有することができる。LK, LK'を作ることができるのは、著作権者だけであるので、ソースが不正に、LK, LK'を作ろうとしても作ることができないので、より安全性を高めることができる。

【0119】以上においては、ソースとシンクにおいて認証を行うようにしたが、例えばパーソナルコンピュータ2には、通常、任意のアプリケーションプログラムをロードして用いることができる。そして、このアプリケーションプログラムとしては、不正に作成したものが使用される場合もある。従って、各アプリケーションプログラム毎に、著作権者から許可を得たものであるか否かを判定する必要がある。そこで、図3に示すように、各アプリケーション部61とライセンスマネージャ62との間においても、上述したように、認証処理を行うようにすることができる。この場合、ライセンスマネージャ62がソースとなり、アプリケーション部61がシンクとなる。

【0120】次に、以上のようにして、認証が行われた後（暗号鍵の共有が行われた後）、暗号鍵を用いて、ソースから暗号化したデータをシンクに転送し、シンクにおいて、この暗号化したデータを復号する場合の動作に

和の演算を意味する。

【0113】すなわち、疑似ランダム発生キーpRNGにステップS105で求めたHを入力することで得られた結果、pRNG(H)と、ステップS106で生成した鍵skのビット毎の排他的論理和を演算することで、鍵SKを暗号化する。

【0114】次に、ステップS108で、ファームウェア20は、eをパーソナルコンピュータ2に伝送する。

【0115】パーソナルコンピュータ2においては、ステップS109でこれを受信し、ステップS110で、次式を演算する。

$$\text{sk}' = e (+) G(LK') (+) \text{pRNG}(LK)$$

【0116】すなわち、DVDプレーヤ1から伝送されてきたe、EEPROM50に記憶されている関数Gに、やはりEEPROM50に記憶されているLK'を適用して得られる値G(LK')、並びに、EEPROM50に記憶されているLK'を、やはりEEPROM50に記憶されている疑似乱数発生関数pRNGに適用して得られる結果pRNG(LK)の排他的論理和を演算し、鍵sk'を得る。

【0117】ここで、次式に示すように、 $\text{sk} = \text{sk}'$ となる。

について説明する。

【0121】図10に示すように、DVDプレーヤ1、あるいは光磁気ディスク装置3のように、内部の機能が一般ユーザに解放されていない装置においては、1394バス11を介して授受されるデータの暗号化と復号の処理は、それぞれ1394インタフェース26または1394インタフェース36で行われる。この暗号化と復号化には、セッションキーSと時変キーiが用いられるが、このセッションキーSと時変キーi（正確には、時変キーiを生成するためのキーi'）は、それぞれファームウェア20またはファームウェア30から、1394インタフェース26または1394インタフェース36に供給される。セッションキーSは、初期値として用いられる初期値キーSsと時変キーiを攪乱するために用いられる攪乱キーSiとにより構成されている。この初期値キーSsと攪乱キーSiは、上述した認証において生成された暗号鍵sk(=sk')の所定のビット数の上位ビットと下位ビットにより、それぞれ構成するようにすることができる。このセッションキーSは、セッション毎に

（例えば、1つの映画情報毎に、あるいは、1回の再生毎に）、適宜、更新される。これに対して、攪乱キーSiとキーi'から生成される時変キーiは、1つのセッション内において、頻繁に更新されるキーであり、例え

ば、所定のタイミングにおける時刻情報などを用いることができる。

【0122】いま、ソースとしてのDVDプレーヤ1から再生出力した映像データを1394バス11を介して光磁気ディスク装置3とパーソナルコンピュータ2に伝送し、それぞれにおいて復号するものとする。この場合、DVDプレーヤ1においては、1394インタフェース26において、セッションキーSと時変キーiを用いて暗号化処理が行われる。光磁気ディスク装置3においては、1394インタフェース36において、セッションキーSと時変キーiを用いて復号処理が行われる。

【0123】これに対して、パーソナルコンピュータ2においては、ライセンスマネージャ62が、セッションキーSのうち、初期値キーSsをアプリケーション部61に供給し、攪乱キーSiと時変キーi（正確には、時変キーiを生成するためのキーi'）を1394インタフェース49（リンク部分）に供給する。そして、1394インタフェース49において、攪乱キーSiとキーi'から時変キーiが生成され、時変キーiを用いて復号が行われ、その復号されたデータは、アプリケーション部61において、さらにセッションキーS（正確には、初期値キーSs）を用いて復号が行われる。

【0124】このように、パーソナルコンピュータ2においては、内部バス51が、ユーザに解放されているので、1394インタフェース49により第1段階の復号だけを行い、まだ暗号の状態としておく。そして、アプリケーション部61において、さらに第2段階の復号を行い、平文にする。これにより、パーソナルコンピュータ2に対して、適宜、機能を付加して、内部バス51において授受されるデータ（平文）をハードディスク47や他の装置にコピーすることを禁止させる。

【0125】このように、この発明の実施の形態においては、内部バスが解放されていないCE装置においては、暗号化、または復号処理は、セッションキーSと時変キーiを用いて1度に行われるが、内部バスが解放されている装置（パーソナルコンピュータ2など）においては、復号処理が、時変キーiを用いた復号処理と、セッションキーSを用いた復号処理に分けて行われる。このように、1段階の復号処理と、2段階に分けた復号処理の両方ができるようにするには、次式を成立させることが必要となる。

$$\text{Dec}(S, \text{Dec}(i, \text{Enc}(\text{algo}(S+i), \text{Data}))) = \text{Data}$$

【0126】なお、上記式において、 $\text{algo}(S+i)$ は、所定のアルゴリズムにセッションキーSと時変キーiを入力して得られた結果を表している。

【0127】図11は、上記式を満足する1394インタフェース26の構成例を表している。この構成例においては、アディティブジェネレータ71により生成したmビットのデータが、シュリンクジェネレータ73に供

給されている。また、LFSR(Linear Feedback Shift Register)72が1ビットのデータを出力し、シュリンクジェネレータ73に供給している。シュリンクジェネレータ73は、LFSR72の出力に対応して、アディティブジェネレータ71の出力を選択し、選択したデータを暗号鍵として加算器74に出力している。加算器74は、入力された平文（1394バス11に伝送するmビットのデータ）と、シュリンクジェネレータ73より供給されるmビットのデータ（暗号鍵）とを加算し、加算した結果を暗号文（暗号化されたデータ）として、1394バス11に出力するようになされている。

【0128】加算器74の加算処理は、 $\text{mod } 2^m$ （ \wedge はべき乗を意味する）で、シュリンクジェネレータ73の出力と平文を加算することを意味する。換言すれば、mビットのデータ同士が加算され、キャリオーバを無視した加算値が出力される。

【0129】図12は、図11に示した1394インタフェース26のさらにより詳細な構成例を表している。ファームウェア20から出力されたセッションキーSのうち、初期値キーSsは、加算器81を介してレジスタ82に転送され、保持される。この初期値キーSsは、例えば、55ワード（1ワードは8ビット乃至32ビットの幅を有する）により構成される。また、ファームウェア20から供給されたセッションキーSのうちの、例えばLSB側の32ビットで構成される攪乱キーSiは、レジスタ85に保持される。

【0130】レジスタ84には、キーi'が保持される。このキーi'は、例えば1394バス11を介して1個のバケットが伝送される毎に、2ビットのキーi'がレジスタ84に供給され、16バケット分の（32ビット分の）キーi'がレジスタ84に保持されたとき、加算器86により、レジスタ85に保持されている32ビットの攪乱キーSiと加算され、最終的な時変キーiとして加算器81に供給される。加算器81は、そのときレジスタ82に保持されている値と加算器86より供給された時変キーiを加算し、その加算結果をレジスタ82に供給し、保持させる。

【0131】レジスタ82のワードのビット数が、例えば8ビットである場合、加算器86より出力される時変キーiが32ビットであるので、時変キーiを4分割して、各8ビットをレジスタ82の所定のアドレス（0乃至54）のワードに加算するようにする。

【0132】このようにして、レジスタ82には、最初に初期値キーSsが保持されるが、その後、この値は、16バケット分の暗号文を伝送する毎に、時変キーiで更新される。

【0133】加算器83は、レジスタ82に保持されている55ワードのうちの所定の2ワード（図12に示されているタイミングの場合、アドレス23とアドレス54のワード）を選択し、その選択した2ワードを加算し

て、シュリンクジェネレータ73に出力する。また、この加算器73の出力は、図12に示すタイミングでは、レジスタ82のアドレス0に転送され、前の保持値に代えて保持される。

【0134】そして、次のタイミングにおいては、加算器83に供給されるレジスタ82の2ワードのアドレスは、アドレス54とアドレス23から、それぞれアドレス53とアドレス22に、1ワード分だけ、図中上方に移動され、加算器83の出力で更新されるアドレスも、図中、より上方のアドレスに移動される。ただし、アドレス0より上方のアドレスは存在しないので、この場合には、アドレス54に移動する。

【0135】なお、加算器81、83、86では、排他的論理和を演算させるようにすることも可能である。

【0136】LFSR72は、例えば、図13に示すように、 n ビットのシフトレジスタ101と、シフトレジスタ101の n ビットのうちの所定のビット（レジスタ）の値を加算する加算器102により構成されている。シフトレジスタ101は、加算器102より供給されるビットを、図中最も左側のレジスタ b_n に保持すると、それまでそこに保持されていたデータを右側のレジスタ b_{n-1} にシフトする。レジスタ b_{n-1} 、 b_{n-2} 、・・・も、同様の処理を行う。そして、さらに次のタイミングでは、各ビットの値を加算器102で加算した値を再び、図中最も左側のビット b_n に保持させる。以上の動作が順次繰り返されて、図中最も右側のレジスタ b_1 から出力が1ビットずつ順次出力される。

【0137】図13は、一般的な構成例であるが、例えば、より具体的には、LFSR72を図14に示すように構成することができる。この構成例においては、シフトレジスタ101が31ビットにより構成され、その図中右端のレジスタ b_1 の値と左端のレジスタ b_{31} の値が、加算器102で加算され、加算された結果がレジスタ b_{31} に帰還されるようになされている。

【0138】LFSR72より出力された1ビットのデータが論理1であるとき、条件判定部91は、アディティブジェネレータ71の加算器83より供給された m ビットのデータをそのままFIFO92に転送し、保持させる。これに対して、LFSR72より供給された1ビットのデータが論理0であるとき、条件判定部91は、加算器83より供給された m ビットのデータを受け付けず、暗号化処理を中断させる。このようにして、シュリンクジェネレータ73のFIFO92には、アディティブジェネレータ71で生成した m ビットのデータのうち、LFSR72が論理1を出力したタイミングのもののみが選択され、保持される。

【0139】FIFO92により保持した m ビットのデータが、暗号鍵として、加算器74に供給され、伝送されるべき平文のデータ（DVDからの再生データ）に加算されて、暗号文が生成される。

【0140】暗号化されたデータは、DVDプレーヤ1から1394バス11を介して光磁気ディスク装置3とパーソナルコンピュータ2に供給される。

【0141】光磁気ディスク装置3は、1394インタフェース36において、1394バス11から受信したデータを復号するために、図15に示すような構成を有している。この構成例においては、シュリンクジェネレータ173にアディティブジェネレータ171の出力する m ビットのデータと、LFSR172が出力する1ビットのデータが供給されている。そして、シュリンクジェネレータ173の出力する m ビットの鍵が、減算器174に供給されている。減算器174は、暗号文からシュリンクジェネレータ173より供給される鍵を減算して、平文を復号する。

【0142】すなわち、図15に示す構成は、図11に示す構成と基本的に同様の構成とされており、図11における加算器74が、減算器174に変更されている点だけが異なっている。

【0143】図16は、図15に示す構成のより詳細な構成例を表している。この構成も、基本的に図12に示した構成と同様の構成とされているが、図12における加算器74が、減算器174に変更されている。その他のアディティブジェネレータ171、LFSR172、シュリンクジェネレータ173、加算器181、レジスタ182、加算器183、レジスタ184、185、加算器186、条件判定部191、FIFO192は、図12におけるアディティブジェネレータ71、LFSR72、シュリンクジェネレータ73、加算器81、レジスタ82、加算器83、レジスタ84、85、加算器86、条件判定部91、およびFIFO92に対応している。

【0144】従って、その動作は、基本的に図12に示した場合と同様であるので、その説明は省略するが、図16の例においては、シュリンクジェネレータ173のFIFO192より出力された m ビットの鍵が、減算器174において、暗号文から減算されて平文が復号される。

【0145】以上のように、1394インタフェース36においては、セッションキー S （初期値キー S_s と攪乱キー S_i ）と時変キー i を用いて、暗号化データが1度に復号される。

【0146】これに対して、上述したように、パーソナルコンピュータ2においては、1394インタフェース49とアプリケーション部61において、それぞれ個別に、2段階に分けて復号が行われる。

【0147】図17は、1394インタフェース49において、ハード的に復号を行う場合の構成例を表しており、その基本的構成は、図15に示した場合と同様である。すなわち、この場合においても、アディティブジェネレータ271、LFSR272、シュリンクジェネレータ273、および減算器274により1394インタフェ

ース49が構成されており、これらは、図15におけるアディティブジェネレータ171、LFSR172、シュリンクジェネレータ173、および減算器174と基本的に同様の構成とされている。ただし、図17の構成例においては、アディティブジェネレータ271に対して、ライセンスマネージャ62から、時変キー*i*を生成するためのキー*i'*と、セッションキー*S*のうち、時変キー*i*を攪乱するための攪乱キー*Si*としては、図15における場合と同様のキーが供給されるが、初期値キー*Ss*としては、全てのビットが0である単位元が供給される。

【0148】すなわち、図18に示すように、初期値キー*Ss*の全てのビットが0とされるので、実質的に、初期値キー*Ss*が存在しない場合と同様に、時変キー*i*だけに基づいて暗号鍵が生成される。その結果、減算器274においては、暗号文の時変キー*i*に基づく復号だけが行われる。また初期値キー*Ss*に基づく復号が行われていないので、この復号の結果得られるデータは、完全な平文とはなっておらず、暗号文の状態になっている。従って、このデータを内部バス51から取り込み、ハードディスク47や、その他の記録媒体に記録したとしても、それをそのまま利用することができない。

【0149】そして、以上のようにして、1394インタフェース49において、ハード的に時変キー*i*に基づいて復号されたデータをソフト的に復号するアプリケーション部61の構成は、図19に示すように、アディティブジェネレータ371、LFSR372、シュリンクジェネレータ373および減算器374により構成される。その基本的構成は、図15に示したアディティブジェネレータ171、LFSR172、シュリンクジェネレータ173、および減算器174と同様の構成となっている。

【0150】ただし、セッションキー*S*のうち、初期値キー*Ss*は、図15における場合と同様に、通常の初期値キーが供給されるが、時変キー*i*を生成するための攪乱キー*Si*とキー*i'*は、それぞれ全てのビットが0である単位元のデータとされる。

【0151】その結果、図20にその詳細を示すように（そのアディティブジェネレータ371乃至FIFO392は、図16におけるアディティブジェネレータ171乃至FIFO192に対応している）、レジスタ384に保持されるキー*i'*とレジスタ385に保持される攪乱キー*Si*は、全てのビットが0であるため、加算器386の出力する時変キー*i*も全てのビットが0となり、実質的に時変キー*i*が存在しない場合と同様の動作が行われる。すなわち、初期値キー*Ss*だけに基づいて暗号鍵が生成される。そして、減算器374においては、このようにして生成された暗号鍵に基づいて暗号文が平文に復号される。上述したように、この暗号文は、1394インタフェース49において、時変キー*i*に基づいて第1段階の復号が行われているものであるため、ここで、初期値キー*Ss*に基づいて第2段階の復号を行うことで、完全な平

文を得ることができる。

【0152】光磁気ディスク装置3においては、以上のようにして暗号文が復号されると、CPU31が、復号されたデータをドライブ35に供給し、光磁気ディスクに記録させる。

【0153】一方、パーソナルコンピュータ2においては、CPU41（アプリケーション部61）が、以上のようにして復号されたデータを、例えばハードディスク47に供給し、記録させる。パーソナルコンピュータ2においては、拡張ボード48として所定のボードを接続して、内部バス51で授受されるデータをモニタすることができるが、内部バス51に伝送されるデータを最終的に復号することができるのは、アプリケーション部61であるので、拡張ボード48は、1394インタフェース49で、時変キー*i*に基づいて復号が行われたデータ（まだ、セッションキー*S*に基づいて復号が行われていないデータ）をモニタすることができたとしても、完全に平文に戻されたデータをモニタすることはできない。そこで、不正なコピーが防止される。

【0154】なお、セッションキーの共有は、例えば、Diffie-Hellman法などを用いて行うようにすることも可能である。

【0155】なお、この他、例えばパーソナルコンピュータ2における1394インタフェース49またはアプリケーション部61の処理能力が比較的低く、復号処理を行うことができない場合には、セッションキーと時変キーのいずれか、あるいは両方をソース側において、単位元で構成するようにし、シンク側においても、これらを単位元で用いるようにすれば、実施的にセッションキーと時変キーを使用しないで、データの授受が可能となる。ただし、そのようにすれば、データが不正にコピーされるおそれが高くなる。

【0156】アプリケーション部61そのものが、不正にコピーしたものである場合、復号したデータが不正にコピーされてしまう恐れがあるが、上述したようにアプリケーション部61をライセンスマネージャ62で認証するようにすれば、これを防止することが可能である。

【0157】この場合の認証方法としては、共通鍵暗号方式の他、公開鍵暗号方式を用いたデジタル署名を利用することができる。

【0158】以上の図11、図12、図15乃至図20に示す構成は、準同形(homomorphism)の関係を満足するものとなっている。すなわち、キー*K*₁、*K*₂がガロアフィールド*G*の要素であるとき、両者の群演算の結果、*K*₁・*K*₂もガロアフィールド*G*の要素となる。そして、さらに、所定の関数*H*について次式が成立する。

$$H(K_1 \cdot K_2) = H(K_1) \cdot H(K_2)$$

【0159】図21は、さらに1394インタフェース26の他の構成例を表している。この構成例においては、セッションキー*S*がLFSR501乃至503に供給さ

れ、初期設定されるようになされている。LFSR 501乃至503の幅 n_1 乃至 n_3 は、それぞれ20ビット程度で、それぞれの幅 n_1 乃至 n_3 は、相互に素になるように構成される。従って、例えば、セッションキーSのうち、例えば、上位 n_1 ビットがLFSR 501に初期設定され、次の上位 n_2 ビットがLFSR 502に初期設定され、さらに次の上位 n_3 ビットがLFSR 503に初期設定される。

【0160】LFSR 501乃至503は、クロッキングファンクション506より、例えば論理1のイネーブル信号が入力されたとき、 m ビットだけシフト動作を行い、 m ビットのデータを出力する。 m の値は、例えば、8、16、32、40などとすることができる。

【0161】LFSR 501とLFSR 502の出力は、加算器504に入力され、加算される。加算器504の加算値のうち、キャリー成分は、クロッキングファンクション506に供給され、sum成分は、加算器505に供給され、LFSR 503の出力と加算される。加算器505のキャリー成分は、クロッキングファンクション506に供給され、sum成分は、排他的論理和回路508に供給される。

【0162】クロッキングファンクション506は、加算器504と加算器505より供給されるデータの組み合わせが、00、01、10、11のいずれかであるので、これらに対応して、LFSR 501乃至503に対して、000乃至111のいずれか1つの組み合わせのデータを出力する。LFSR 501乃至503は、論理1が入力されたとき、 m ビットのシフト動作を行い、新たな m ビットのデータを出力し、論理0が入力されたとき、前回出力した場合と同一の m ビットのデータを出力する。

【0163】排他的論理和回路508は、加算器505の出力するsum成分とレジスタ507に保持された時変キー i の排他的論理和を演算し、その演算結果を排他的論理和回路509に出力する。排他的論理和回路509は、入力された明文と、排他的論理和回路508より入力された暗号鍵の排他的論理和を演算し、演算結果を暗号文として出力する。

【0164】図22は、光磁気ディスク装置3における1394インタフェース36の構成例を表している。この構成例におけるLFSR 601乃至排他的論理和回路609は、図21におけるLFSR 501乃至排他的論理和回路509と同様の構成とされている。従って、その動作も、基本的に同様となるので、その説明は省略する。ただし、図21の構成例においては、暗号化処理が行われるのに対して、図22の構成例においては、復号処理が行われる。

【0165】図23は、パーソナルコンピュータ2の1394インタフェース49の構成例を表している。この構成例におけるLFSR 701乃至排他的論理和回路709も、図22における、LFSR 601乃至排他的論理和回路

609と同様の構成とされている。ただし、LFSR 701乃至703に初期設定されるセッションキーSは、全てのビットが0の単位元とされている。従って、この場合、実質的にレジスタ707に保持された時変キー i だけに対応して復号化処理が行われる。

【0166】図24は、パーソナルコンピュータ2のアプリケーション部61の構成例を表している。この構成例におけるLFSR 801乃至排他的論理和回路809は、図22における、LFSR 601乃至排他的論理和回路609と基本的に同様の構成とされている。ただし、レジスタ807に入力される時変キー i が、全てのビットが0である単位元とされている点のみが異なっている。従って、この構成例の場合、セッションキーSだけに基いて暗号鍵が生成され、復号処理が行われる。

【0167】なお、図19、図20、および図24に示す処理は、アプリケーション部61において行われるので、ソフト的に処理されるものである。

【0168】ところで、何らかの理由でlicense_keyが盗まれてしまったような場合には、適宜、これを変更（更新）するようにすることができる。勿論、このlicense_keyが実際に盗まれなくても、盗まれるおそれがある場合には、所定の周期で、これを更新するようにすることができる。この場合、例えば、DVD（ディスク）内に、そのとき有効とされるlicense_keyのバージョン（この実施の形態の場合、hash関数の適用回数）が記録される。また、対象となる操作が、DVDプレーヤではなく、例えば衛星を介して伝送されてくる情報を受信する受信装置である場合には、衛星から、そのバージョンの情報が受信装置に向けて伝送される。

【0169】図25と図26は、DVDプレーヤにおいて、license_keyを更新する場合の処理例を表している。なお、この実施の形態の場合には、図4に示した情報が、DVDプレーヤ1のEEPROM 27とパーソナルコンピュータ2のEEPROM 50に記憶されている他、EEPROM 50にはhash関数も記憶されている。

【0170】最初に、ステップS151において、ソースとしてのDVDプレーヤ1は、シンクとしてのパーソナルコンピュータ2に対して、IDを要求する。パーソナルコンピュータ2は、ステップS152で、このID要求信号を受け取ると、ステップS153で、自分自身のIDをDVDプレーヤ1に送出する。DVDプレーヤ1は、ステップS154で、このIDを受信する。

【0171】次に、DVDプレーヤ1は、ステップS155で、次式から鍵 lk を演算する。

$lk = \text{hash}(ID \parallel \text{service_key})$

【0172】以上の処理は、図4のステップS1乃至S5の処理と同様の処理である。

【0173】次に、ステップS156に進み、DVDプレーヤ1は、ステップS155で演算した鍵 lk が有効なバージョンのものであるか否かを判定する。すなわち、上

述したように、DVDには、現在有効なlicense_key (=lk) のバージョン (hash関数の適用回数) が記録されている。ステップS155で生成した鍵lkは、hash関数を1回適用して求めたものである。このhash関数の適用回数がバージョンで規定されている回数と等しくない場合、鍵lkは無効と判定される。この場合、ステップS157に進み、DVDプレーヤ1は、更新回数 (演算回数) を示す変数gに1を初期設定し、lk_gにlkを設定する。そして、ステップS158において、現在の鍵lk_gにhash関数を1回適用し、新たな鍵lk_{g+1}を演算する。すなわち、次式を演算する。

$$lk_{g+1} = \text{hash}(lk_g)$$

【0174】ステップS159では、ステップS158で求められた鍵lk_{g+1}が有効であるか否かを判定する。すなわち、バージョンに規定された回数と同一の回数だけhash関数を適用したか否かを判定する。適用回数がバージョンに規定されている回数に達していないとき、ステップS160に進み、DVDプレーヤ1は、変数gを1だけインクリメントする。そして、ステップS158に戻り、再び現在の鍵lk_gにhash関数を適用し、演算する。

【0175】以上のようにして、バージョンに規定されている回数とhash関数を適用した回数が等しくなるまで、同様の処理が繰り返し実行される。

【0176】なお、この繰り返し回数には、例えば100回など上限値を設けるようにしてもよい。

【0177】ステップS159で、バージョンに対応する回数だけhash関数が適用されたと判定された場合 (有効な鍵lk_{g+1}が得られたと判定された場合)、並びに、ステップS156で、鍵lkが有効であると判定された場合、ステップS161に進み、上述した場合と同様に、暗号鍵skを生成する。ステップS162では、ステップS155またはステップS158で生成した鍵lk_gを鍵として、暗号鍵skを暗号化する。すなわち、次式を演算する。

$$e = \text{Enc}(lk_g, sk)$$

【0178】次に、ステップS163において、DVDプレーヤ1は、パーソナルコンピュータ2に対して、ステップS162で暗号化したデータeと、hash関数の適用回数を表す変数gを送信する。パーソナルコンピュータ2においては、ステップS164でこれを受信すると、ステップS165で、パーソナルコンピュータ2におけるhash関数の適用回数を表す変数wに1を初期設定する。次に、ステップS166に進み、ステップS164で受信した変数gと、ステップS165で設定した変数wの値が等しいか否かを判定する。両者が等しくない場合、ステップS167に進み、パーソナルコンピュータ2のEEPROM50に記憶されているlicense_keyにhash関数を適用して、新たなlicense_key_{w+1}を次式から求める。

$$\text{license_key}_{w+1} = \text{hash}(\text{license_key}_w)$$

【0179】次に、ステップS168に進み、wを1だけインクリメントして、ステップS166に戻る。ステップS166で再び変数gと変数wが等しいか否かを判定し、両者が等しいと判定されるまで、ステップS167、S168の処理が繰り返し実行される。

【0180】ステップS166で、変数gが変数wと等しいと判定された場合 (現在有効なlicense_key_wが得られた場合)、ステップS169に進み、次式から暗号鍵sk'が演算される。

$$sk' = \text{Dec}(\text{license_key}_w, e)$$

【0181】以上のように、license_key (=lk) を適宜更新するようにすれば、より安全性を高めることができる。

【0182】なお、図25と図26に示した処理例の場合、バージョンを表す変数gをソース側からシンク側に伝送するようにしたが、これを伝送しないで、license_keyを更新することも可能である。この場合、図25の処理に続いて、図27に示す処理が実行される。

【0183】すなわち、この例の場合、ステップS163で、DVDプレーヤ1からパーソナルコンピュータ2に対して、暗号化データeだけが伝送され、バージョンを表す変数gは伝送されない。ステップS164で、パーソナルコンピュータ2がこの暗号化データeを受信すると、ステップS165で、この暗号化データeをlicense_keyを用いて復号する処理が、次式で示すように実行される。

$$sk' = \text{Dec}(\text{license_key}, e)$$

【0184】また、ステップS166で、DVDプレーヤ1は、ステップS161で生成した暗号鍵skを用いて、送出するデータを暗号化し、伝送する。パーソナルコンピュータ2は、ステップS167でこれを受信すると、ステップS168で、ステップS165で求めた暗号鍵sk'を用いて、復号する処理を実行する。次に、ステップS169で、復号した結果得られたデータが正しいか否かを判定する。この判定は、例えばMPEG方式のTS (Transport Stream) パケットが受信されている場合には、そのヘッダ部分に、同期合わせのためのコード (16進表示で47) が挿入されているので、このコードが完全であるか否かをチェックすることで行うことができる。

【0185】正しい復号ができなかった場合には、ステップS170に進み、パーソナルコンピュータ2は、次式に従って、license_keyを更新する。

$$\text{license_key} = \text{hash}(\text{license_key})$$

【0186】次に、ステップS171に進み、ステップS170で求めたlicense_keyを鍵として、ステップS164で受信した暗号化データeを、次式に従って復号する。

$$sk' = \text{Dec}(\text{license_key}, e)$$

【0187】そして、ステップS168に戻り、ステッ

ブS171で求めた暗号鍵sk'を用いて、ステップS167で受信した暗号化されているデータを復号する。ステップS169では、正しい復号が行われたか否かを再び判定する。以上のようにして、ステップS169で正しい復号が行われたと判定されるまで、ステップS170, S171, S168の処理が繰り返し実行される。

【0188】以上のようにしても、license_keyを更新することができる。

【0189】また、ソース側における暗号鍵の生成処理とシンク側における復号鍵（暗号鍵）の生成処理は、それぞれ処理対象とするデータと同期を取る必要がある。

【0190】例えば、図21に示すソース側の1394インタフェース26において、LFSR501乃至排他的論理和回路508で生成する暗号鍵と、これを用いて暗号化するデータとしての平文の位相関係が、図22に示すシンク側の1394インタフェース36において、LFSR601乃至排他的論理和回路608で生成される暗号鍵と、この暗号鍵を用いて復号される暗号文の位相関係と一致している必要がある。そこで、図示は省略しているが、図21の1394インタフェース26においては、入力される平文に同期して暗号鍵が生成されるようになされており、また、図22の1394インタフェース36においては、入力される暗号文に同期して、暗号鍵が生成されるようになされている。

【0191】従って、例えばソース側から1394バス11を介してシンク側に送出された暗号文を構成するパケットや所定のビットが何らかの理由で欠落してしまったような場合、ソース側における平文と暗号鍵の位相に対応する位相を、シンク側の暗号文と暗号鍵において保持することができなくなる。そこで、両者の位相関係が所定のタイミングで確実に更新される（初期化される）ようにすることができる。図28は、このような処理を行う場合の構成例を表している。

【0192】すなわち、この構成例においては、排他的論理和回路901が、乱数発生器903が発生する乱数と、入力される平文の排他的論理和を演算し、排他的論理和回路904と演算回路902に出力するようになされている。演算回路902にはまた、セッションキーSも入力されている。演算回路902は、セッションキーSと排他的論理和回路901の出力Ciに対して、所定の演算を施して、その演算結果を乱数発生器903に出力するようになされている。

【0193】排他的論理和回路904は、排他的論理和回路901より入力されたデータと、時変キーiの排他的論理和を演算し、暗号文として1394バス11に出力するようになされている。

【0194】同様に、シンク側においては、排他的論理和回路911が1394バス11を介して入力される暗号文と、時変キーiの排他的論理和を演算し、排他的論理和回路912と演算回路913に出力している。演算

回路913には、セッションキーSも入力されている。演算回路913は、排他的論理和回路911からの入力Ciと、セッションキーSに対して所定の演算を施して、その演算結果を乱数発生器914に出力している。乱数発生器914は、演算回路913から入力される値を初期値として乱数を発生し、発生した乱数を排他的論理和回路912に出力している。排他的論理和回路912は、排他的論理和回路911より供給される暗号文と、乱数発生器914より入力される乱数との排他的論理和を演算し、暗号文を復号して平文として出力するようになされている。

【0195】乱数発生器903は、例えば図29に示すように、LFSR931乃至クロッキングファンクション936により構成されている。これらは、図21に示したLFSR501乃至クロッキングファンクション506と同様の構成とされている。

【0196】なお、図示は省略するが、シンク側の乱数発生器914も、図29に示した構成と同様に構成されている。

【0197】また、ソース側の演算回路902とシンク側の演算回路913は、それぞれ図30のフローチャートに示すような処理を実行するように構成されている。

【0198】次に、その動作について説明する。

【0199】ソース側の演算回路902は、排他的論理和回路901からの入力Ciに、所定の関数fを適用して、Viを演算する機能、すなわち、次式を演算する機能を有している。

$$V_i = f(S, C_i)$$

【0200】ステップS201では、上記式におけるCiに0を初期設定して次式が演算される。

$$V_0 = f(S, 0)$$

【0201】演算回路902は、ステップS201で演算した値を、ステップS202で乱数発生器903に出力する。乱数発生器903では、演算回路902の出力V0が、LFSR931乃至933に入力され、初期設定される。そして、図21に示した場合と同様にして、乱数が生成され、加算器935から出力される。この乱数が排他的論理和回路901に供給される。

【0202】排他的論理和回路901は、この乱数と入力された平文との排他的論理和を演算し、演算結果Ciを演算回路902に供給する。

【0203】演算回路902においては、次に、ステップS203において、変数iに1が初期設定され、ステップS204において、排他的論理和回路901から入力されたデータがCiに設定される。

【0204】次に、ステップS205に進み、演算回路902は、次式を演算する。

$$V_i = f(S, C_i) + V_{i-1}$$

【0205】いまの場合、i=1であるから、次式が演算される。

$$V_1 = f(S, C_1) + V_0$$

【0206】次に、ステップS206に進み、いま取り込まれたデータ C_i が予め設定してある所定の値 T と等しいか否かが判定される。両者の値が等しくない場合、ステップS207に進み、変数 i が1だけインクリメントされた後、ステップS204に戻る。すなわち、いまの場合、 $i=2$ とされ、次に入力されたデータが C_2 に設定される。

【0207】次に、ステップS205で次式が演算される。

$$V_2 = f(S, C_2) + V_1$$

【0208】ステップS206では、 C_2 の値が所定の値 T と等しいか否かが判定され、等しくなければ、ステップS207に進み、変数 i が1だけインクリメントされ、再びステップS204以降の処理が実行される。

【0209】ステップS206において、 C_i の値が所定の値 T と等しいと判定された場合、ステップS208に進み、ステップS205で演算された値 V_i が乱数発生器903に出力される。乱数発生器903では、ステップS202で説明した場合と同様に、この値がLFSR931乃至933に初期値として設定される。そして、この初期値に対応する乱数が加算器935から出力される。

【0210】演算回路902は、 V_i を乱数発生器903に出力した後、ステップS203に戻り、変数 i を1に初期設定した後、それ以降の処理を繰り返し実行する。

【0211】いま、例えば T の値が8ビットで表されるものとし、 C_i の値は、その発生確率が均等であるとする、256(=2⁸)回に1回の割合で、 C_i の値は T と等しくなることになる。従って、乱数発生器903の発生する乱数は、256回に1回の割合で初期化(更新)されることになる。

【0212】排他的論理和回路901より出力されたデータは、排他的論理和回路904に入力され、時変キー i との排他的論理和が演算された後、暗号文として1394バス11に出力される。

【0213】シンク側においては、排他的論理和回路911が、1394バス11を介して入力された暗号文と、時変キー i の排他的論理和を演算し、その演算結果 C_i を、演算回路913に出力している。演算回路913は、上述したソース側の演算回路902と同様の処理を実行し、256回に1回の割合で、乱数発生器914に初期値 V_i を供給する。乱数発生器914は、入力された値 V_i を初期値として乱数を発生し、発生した乱数を排他的論理和回路912に出力する。排他的論理和回路912は、入力された乱数と、排他的論理和回路911より入力された暗号化されているデータとの排他的論理和を演算し、演算結果を平文として出力する。

【0214】このように、演算回路913は、排他的論理和回路911が暗号データを256回出力すると1回の割合で初期値を発生する。従って、シンク側に139

4バス11を介して入力される暗号データに欠落が生じたとしても、シンク側の暗号文と乱数の位相関係は、暗号データ256個に1個の割合で初期化されるため、その時点で位相関係が回復することになる。

【0215】なお、演算回路902または演算回路913が初期値を出力するのは、 $T=C_i$ となった場合であるから、256回に1回の割合で定期的に初期値が出力されるのではなく、平均すると確率的にそのようになるにすぎない。

【0216】なお、送信または受信した暗号データの数をカウントして、同様の処理を実行させるようにすることも可能であるが、そのようにすると、1394バス11上でデータが欠落すると、ソース側におけるデータのカウンタ値とシンク側におけるデータのカウンタ値とが異なる値となってしまう、結局、両者の同期を取ることができなくなってしまう。そこで、上記した実施の形態のようにするのが好ましい。

【0217】また、乱数発生器903または乱数発生器914に供給する初期値としては、排他的論理和回路901または911の出力するデータ C_i をそのまま利用することも可能である。しかしながら、このデータ C_i は、1394バス11上を伝送されるデータであり、盗まれるおそれがある。そこで、データ C_i を初期値として直接利用せず、これに対して所定の演算を施すことによって生成された値 V_i を初期値とするようにすれば、より安全性を高めることができる。

【0218】ところで、IEEE1394バス11のデータ転送方式には、asynchronous転送とisochronous転送の2つの方法がある。このうちのasynchronous転送は、2つの機器間での1対1の転送であり、isochronous転送は、1つの機器から1394バス11上のすべての機器に対する同報通信であると考えることができる。従って、例えば図4などに示した認証、鍵共有プロトコルの通信は、同報する必要がないので、asynchronous転送で行われるのが普通である。

【0219】いま、図4の認証、鍵共有プロトコルにおいて、例えばパーソナルコンピュータ2が不正な機器で、license_keyを持っていない場合にも、DVDプレーヤ1から e を送ってもらうことができる。ここで e は、セッションキー sk を鍵 lk で暗号化した暗号文である。不正な機器であるパーソナルコンピュータ2は、license_keyを持っていないので、 e を復号して正しい sk を得ることはできないが、 e が暗号解読に用いられるおそれがある。

【0220】なんらかの理由によりパーソナルコンピュータ2がセッションキー sk を得た場合には、平文 sk と鍵 lk を用いて暗号化した暗号文 e の両方を手に入れたことになる。その結果、これらが暗号解読に用いられるおそれがある。さらにいえば、攻撃者が平文と暗号文の組をたくさん知るほど、一般的に暗号解読が容易になる。

【0221】また、不正なパーソナルコンピュータ2がIDをDVDプレーヤ1に教える際に、虚偽のIDを教え、DVDプレーヤ1は、この虚偽のIDに基づいて鍵 k を計算し、これに基づいてセッションキー sk を暗号化して送り返してしまう。このような操作を繰り返すことにより、パーソナルコンピュータ2は、ひとつの平文 sk を複数の暗号鍵 k でそれぞれ暗号化した、複数の暗号文 e を手に入れることができることになる。

【0222】図31は、この点を考慮して、シンク機器が不正な機器であった場合には、あるセッションキー sk を鍵 k で暗号化した暗号文 e が2つ以上は、そのシンク機器にわたらないようにする処理例を表している。この図31における処理は、基本的に、図4に示した処理と同様であるが、ソース機器がシンク機器に対してIDを要求する以前に、いくつかの処理が設けられている。

【0223】すなわち、図31の処理例においては、ステップS201において、シンク機器としてのパーソナルコンピュータ2が、ソース機器としてのDVDプレーヤ1に対して認証プロトコルの開始を要求する認証要求を転送する。この認証要求は、プロトコルの他の転送と同様に、asynchronous転送によって行われる。

【0224】IEEE1394バス11では、それに接続されているそれぞれの機器が、バスリセット時に固有のノード番号が割り当てられ、各機器は、このノード番号によって、送信機器、受信機器の指定、識別を行うようにしている。

【0225】図32は、asynchronousパケットのひとつである、write request for data quadletパケットのフォーマットを示している。同図におけるdestination_IDは、受信機器のノード番号を示し、source_IDは、送信機器のノード番号を示している。認証要求を表すパケットでは、quadlet_dataの位置に、あらかじめ定められた認証要求を表すデータが挿入される。

【0226】DVDプレーヤ1は、ステップS202で認証要求を表すasynchronousパケットを受け取ると、そのパケットを送信した機器のノード番号であるsource_IDを読み取る。そして、ステップS203において、DVDプレーヤ1は、現在のセッションキー sk に関して、このノード番号の機器に対して、暗号文 e を既に送っているか否かを判定する。暗号文 e を既に送ったことがある場合には、DVDプレーヤ1は、パーソナルコンピュータ2に対する認証プロトコルの処理を終了する。これに対して、パーソナルコンピュータ2に対して、まだ暗号文 e をまだ送信したことがない場合には、さらにステップS204以降の認証プロトコルが実行される。

【0227】このステップS204乃至ステップS213の処理は、図4におけるステップS1乃至ステップS10の処理と同様の処理である。

【0228】このような処理が行われた後、DVDプレーヤ1は、ステップS214において、ステップS213

で読み取ったパーソナルコンピュータ2のノード番号を、EEPROM27に記憶する。このノード番号は、DVDプレーヤ1が現在のセッションキー sk を使い続ける限り保存される。そして、セッションキー sk を変更するとき、消去される。

【0229】以上のようにすることにより、ひとつのシンク機器がひとつのセッションキー sk について得られる暗号文 e の数は高々ひとつであるプロトコルを構成することができる。これにより、より安全性を高めることが可能となる。

【0230】ところで、図4の認証プロトコルのステップS7においては、ソース機器がシンク機器に対して送るべきセッションキー sk を鍵 k を用いて暗号化し、 e を生成している。この暗号アルゴリズムのうちで広く用いられているものにブロック暗号がある。このブロック暗号は、平文の一定の長さのブロックを単位として暗号化処理を行うものであり、よく知られているものとして、DES暗号がある。このDES暗号は、平文の64ビットのブロックを64ビットの暗号文に変換する暗号アルゴリズムである。

【0231】いま、図4のステップS7において、使用する暗号アルゴリズムを n ビットの平文を n ビットの暗号文に変換する n ビットブロック暗号とし、セッションキー sk のビット長を n ビットとする。また、 n ビットのセッションキー sk を、この暗号アルゴリズムに入力し、鍵 k を用いて変換された結果の n ビットを、そのまま e とするものとする。

【0232】この場合、ソース機器が所定のシンク機器に対して、以前に使用したことのあるセッションキー sk を送ろうとした場合、暗号アルゴリズムの入力と鍵が同一であるため、 e も以前使われたものと同じになり、例えば e を盗聴した不正者に、以前と同じセッションキー sk が使われているという情報を与えてしまうことになる。

【0233】図33は、この点を考慮した認証プロトコルの例を表している。図33におけるステップS221乃至ステップS226までの処理は、図4におけるステップS1乃至ステップS6の処理と同様の処理であるので、ここではその説明を省略する。

【0234】ステップS227において、ソース機器は n ビットの乱数 r を生成し、ステップS228において、次式に従って、暗号 r とセッションキー sk の連結を鍵 k で暗号化する。

$$e = \text{Enc}(k \parallel r \parallel sk)$$

【0235】このとき、CBCモードという暗号モードが用いられる。図34は、このCBCモードの構成を表している。同図において、左側半分が暗号化処理を、右側半分が復号化処理を、それぞれ表している。レジスタ1003とレジスタ1012には、同一の値の初期値IVが格納されている。この初期値IVは、システム全体で固

定されている。

【0236】暗号化処理においては、まず、平文の n ビットの第1ブロックがレジスタ1003の値 IV と排他的論理和演算回路1001において排他的論理和演算され、その結果が暗号器1002に入力される。暗号器1002の n ビットの暗号文は、第1ブロックとして通信路に送信されるとともに、レジスタ1003に格納される。

【0237】平文の n ビットの第2ブロックが入力されると、この第2ブロックは、レジスタ1003に格納されている n ビットの暗号文の第1ブロックと排他的論理和回路1001において排他的論理和演算される。その演算結果は、暗号器1002に入力され、暗号化される。暗号器1002の出力する n ビットの暗号文は、第2ブロックの暗号文として通信路に送信されるとともに、レジスタ1003に格納される。以上の処理が繰り返し実行される。

【0238】一方、復号側においては、通信路を介して伝送されてきた暗号文の第1ブロックが復号器1011により復号され、排他的論理和回路1013において、レジスタ1002に保持されている初期値 IV と排他的論理和演算され、平文の第1ブロックが生成される。

【0239】通信路を介して伝送されてきた第1ブロックの暗号文は、レジスタ1012に保持される。そして、通信路を介して第2ブロックの暗号文が供給されてきたとき、復号器1011が、この第2ブロックの暗号文を復号し、排他的論理和回路1013に供給する。排他的論理和回路1013は、復号器1011の出力する第2ブロックの復号結果とレジスタ1002に保持されている第1ブロックの暗号文との排他的論理和を演算し、第2ブロックの平文を生成する。

【0240】第2ブロックの暗号文はまた、レジスタ1012に保持される。

【0241】以上のような処理が繰り返し実行され、復号化処理が行われる。

【0242】なお、CBCモードに関しては、Bruce Schneier著のApplied Cryptography (Second edition)に詳述されている。

【0243】図33に戻って、ステップS228においては、 n ビットの乱数 r を平文の第1ブロックとし、セッションキー sk を平文の第2ブロックとして暗号プロトコルに入力する。従って、第1ブロックの乱数 r は、レジスタ1003に保持されている初期値 IV と排他的論理和演算された後、暗号器1002で鍵 lk を用いて暗号化される。従って、暗号器1002から、 $Enc(lk, r(+))IV$ が出力される。

【0244】この暗号器1002の出力がレジスタ1003に保持され、第2ブロックの平文としてのセッションキー sk が入力されてきたとき、排他的論理和回路1001で排他的論理和が演算される。従って、このとき、

暗号器1002の出力は、 $Enc(lk, sk(+))Enc(lk, r(+))IV$ となる。

【0245】ソース機器は、ステップS229において、2つのブロックの連結を次式で示すように演算し、シンク機器に送信する。

$$e = Enc(lk, r(+))IV \parallel Enc(lk, sk(+))Enc(lk, r(+))IV$$

【0246】シンク機器側においては、ステップS230で送信されてきた e を受け取り、ステップS231において、EEPROM50に記憶されているlicense_keyを用いて、これを復号する。復号して得られた結果のうち、第1ブロックを r' とし、第2ブロックを sk' とする。

【0247】以上のようにして、シンク機器が正しいlicense_keyを持っている場合においてのみ、 $sk = sk'$ となり、ソース機器側とシンク機器側において、セッションキーを共有することができる。

【0248】上述の e の式が意味するところは、同一のセッションキー sk が2度以上用いられたとしても、乱数 r が変化すれば、 e も変化するということである。このため、 e を盗聴されたとしても、盗聴者にはセッションキー sk が同一であるかどうか不明であるため、安全性を高めることができる。

【0249】なお、ブロック暗号の利用モードとしてよく知られているものに、上記したCBCモードの他、ECBモード、CFBモード、OFBモードなどがある。このうちの後者の2つはフィードバックを用いているので、図33に示した処理に用いることができる。また、これ以外の暗号モードについても、フィードバックを用いるモードのものは、適用することが可能である。ブロック暗号の利用モードについても、上記したApplied Cryptography (Second edition)に詳述されている。

【0250】ところで、図4に示した処理例においては、ソース機器がシンク機器に対してセッションキー sk を暗号化した暗号文 e を送り、正当なシンク機器のみが、この暗号文 e を正しく復号してセッションキー sk を得られるので、実質的にソース機器がシンク機器を認証していることになる。この方式では、ソース機器の認証は行われていない。その結果、不正なソース機器がシンク機器に対して、でたらめなデータを e として送った場合においても、シンク機器は、それを復号した結果をセッションキー sk として受け入れてしまうことが起こりえる。そこで、これを防止するために、図35に示すような、処理を行うことができる。

【0251】この図35の例においては、ステップS241において、シンク機器としてのパーソナルコンピュータ2が、あらかじめ定められているビット数（例えば64ビット）の乱数 r を生成し、ステップS242において、これをソース機器としてのDVDプレーヤ1に送信する。DVDプレーヤ1は、ステップS243において、この乱数 r を受信し、ステップS244において、パー

ソナルコンピュータ 2 に対して、ID を要求する。ステップ S 2 4 5 でこれを受信したパーソナルコンピュータ 2 は、ステップ S 2 4 6 において、EEPROM 5 0 に記憶されている ID を読み出し、DVD プレーヤ 1 に送信する。DVD プレーヤ 1 は、ステップ S 2 4 7 で、この ID を受信する。

【0252】DVD プレーヤ 1 はまた、ステップ S 2 4 8 において、次式に基づいて、鍵 lk を生成する。

$lk = \text{hash}(ID \parallel \text{service_key})$

【0253】また、DVD プレーヤ 1 は、ステップ S 2 4 9 において、セッションキー sk を生成する。

【0254】さらに、ステップ S 2 5 0 において、DVD プレーヤ 1 は、次式に基づいて、e を生成する。

$e = \text{Enc}(lk, r \parallel sk)$

【0255】このようにして生成された e は、ステップ S 2 5 1 において、DVD プレーヤ 1 からパーソナルコンピュータ 2 に送信される。

【0256】なお、このときの暗号化モードとしては、CBC モードなど、フィードバックを利用するものが使用される。

【0257】ステップ S 2 5 2 で、e を受信したパーソナルコンピュータ 2 は、ステップ S 2 5 3 において、e を license_key を用いて復号した結果を、r' と sk' の連結 $r' \parallel sk'$ とする。

【0258】このとき、r' のビット数は、あらかじめ定められている r のビット数と同じビット数になるようにする。

【0259】次に、ステップ S 2 5 4 において、パーソナルコンピュータ 2 は、 $r = r'$ が成り立つかどうかを検査する。 $r = r'$ が成立する場合、パーソナルコンピュータ 2 は、DVD プレーヤ 1 が正当な機器であることを確認し、sk' をセッションキーとして受理する。これは、license_key を用いて復号した結果の r' が r と等しくなるような暗号文 e を作成することができるのは、正しい鍵 lk を作成することが可能な機器だけであるからである。

【0260】これに対して、 $r = r'$ が成立しない場合には、パーソナルコンピュータ 2 は、DVD プレーヤ 1 は、正当な機器ではないと判断し、sk' を破棄する。

【0261】以上のように認証方式を構成することで、シンク機器がソース機器を認証することが可能となる。また、このように認証することにより、図 4 の処理例において実現されていた、正当なシンク機器だけが正しいセッションキーを得ることができる、という特徴も満たしている。

【0262】図 3 6 には、上記と同じ、シンク機器がソース機器の正当性を確認できる認証方式の、別の処理例が示されている。本処理例において、ステップ S 2 6 1 からステップ S 2 6 6 の処理は、図 4 のステップ S 1 からステップ S 6 と同様であるので、その説明は省略す

る。

【0263】ステップ S 2 6 7 において、DVD プレーヤ 1 は時刻情報を T とする。この時刻情報として具体的には、例えば、IEEE 1394 規格において定められている、32 ビットの CYCLE_TIME レジスタの値を使用する。

【0264】CYCLE_TIME レジスタは IEEE 1394 バス上における機器の時刻情報を一定にするために用いられ、バス上に 1 つあるサイクルマスターと呼ばれる機器からの同報パケットによって各機器の CYCLE_TIME レジスタが一樣に更新される。さらにバス上に共通の 24.576MHz のクロックによっても CYCLE_TIME レジスタが 1 ずつ加算されるので、レジスタは約 40 ナノ秒毎に 1 度加算される。このことにより、バス上の各機器間の時計合わせが行える。

【0265】DVD プレーヤ 1 は、ステップ S 2 6 8 において、 $T \parallel sk$ を lk で暗号化して e を得て、ステップ S 2 6 9 でパーソナルコンピュータ 2 に送信する。暗号化の際の暗号モードとしては、CBC モードなど、フィードバックを利用するものが使用される。

【0266】パーソナルコンピュータ 2 はステップ S 2 7 0 で e を受信し、ステップ S 2 7 1 で license_key を用いてこれを復号し、その結果を $T' \parallel sk'$ とおく。この際、T' の部分のビット数を 32 ビットとする。

【0267】ステップ S 2 7 2 で、T' の正当性を検査する。この検査では、パーソナルコンピュータ 2 自身が持つ CYCLE_TIME レジスタの値と、T' の値を比較し、その差が例えば 100 ミリ秒以内であればこれを正しいとし、それを越えていれば不正であるとする。

【0268】この検査に合格した場合、パーソナルコンピュータ 2 は DVD プレーヤ 1 が正当な機器であると判断して、sk' をセッションキーとして受理し、不合格の場合にはパーソナルコンピュータ 2 は DVD プレーヤ 1 が不正な機器であるとして sk' を破棄する。これは、license_key を用いて復号した結果が正しい T' となるような暗号文を生成できるのは、正しい lk を作れる機器だけであるためである。

【0269】以上のように認証方式を構成することにより、シンク機器がソース機器を認証できる方式とすることが可能となる。加えて、この方式でも、図 4 の処理例で実現されていた、正当なシンク機器だけが正しいセッションキーを得ることができる、という特徴も満たしている。

【0270】図 4 の処理例においては、license_key を所有している正当なシンク機器のみが e を正しく復号して $sk = sk'$ なる sk' を得ることが出来るので、実質的にソース機器がシンク機器を認証する方式を構成している。しかし、この方式ではシンク機器が不正デバイスである場合にも、セッションキーを lk を用いて暗号化した暗号文 e を得ることができてしまう。不正デバイスであるシンク機器は e を用いて暗号解読を行ってセッションキー

skを得ようとする可能性がある。

【0271】この問題に対し、図37に示す認証方式の処理例では、ソース機器がシンク機器を正当なものであると確認した後に、セッションキーを暗号化した暗号文を送るようにしている。図37の処理例を説明する。以下の処理例において、暗号化を行う際の暗号モードは、CBCモードなど、フィードバックを利用するものを使用する。

【0272】ステップS281からステップS285は図4の処理例のステップS1からステップS5と同様であるので説明を省略する。ステップS286において、DVDプレーヤ1はあらかじめ定められたビット数（例えば64ビット）の乱数 r_1 と r_2 を生成し、その連結を M_1 とする。ステップS287において、 M_1 を鍵 lk で暗号化して X を作り、ステップS288で X をパーソナルコンピュータ2に送る。

【0273】ステップS289で X を受け取ったパーソナルコンピュータ2は、ステップS290で、 $license_key$ を用いてこれを復号し、あらかじめ定められたビット数（例えば64ビット）ごとに分割して $r_1' || r_2'$ とする。次にステップS291であらかじめ定められたビット数（例えば64ビット）の乱数 r_3 を生成し、ステップS292で、 r_3 と r_2' を連結して M_2 を得る。ステップS293で、 M_2 を $license_key$ を用いて暗号化して Y を得、ステップS294で、 Y をDVDプレーヤ1に送信する。

【0274】ステップS295で Y を受信したDVDプレーヤ1は、ステップS296で lk を用いてこれを復号し、あらかじめ定められたビット数（例えば64ビット）ごとに分割して $r_3' || r_2''$ とする。ステップS297において、 r_2'' と先に送った r_2 が等しいかどうかを検査する。この検査に失敗した場合、DVDプレーヤ1はパーソナルコンピュータ2が正当な機器ではないと判断して認証プロトコルをそこで終了する。この検査に合格した場合、ステップS298においてDVDプレーヤ1はセッションキー sk を生成し、ステップS299において、 r_3' と sk を連結することにより M_3 を得る。ステップS300で M_3 を鍵 lk を用いて暗号化して暗号文 Z を得て、ステップS301でこれをパーソナルコンピュータ2に送信する。

【0275】パーソナルコンピュータ2はステップS302で Z を受信し、ステップS303で Z を $license_key$ で復号し、あらかじめ定められたビット数（例えば64ビット）ごとに分割して $r_3'' || sk'$ とする。ステップS304において、 r_3'' が先に送信した r_3 と等しいかどうかを検査する。この検査に失敗した場合、パーソナルコンピュータ2はDVDプレーヤ1が正当な機器ではないと判断して認証プロトコルを終了する。この検査に合格した場合、パーソナルコンピュータ2は sk' をセッションキー sk として受理する。

【0276】以上のように認証プロトコルを構成するこ

とにより、ソース機器はシンク機器が正当な機器であることを認証した後にセッションキー sk を暗号化した暗号文をシンク機器に対して送ることができる。また本処理例では図33に示した処理例と同様に、たとえソース機器が以前使ったものと同じセッションキー sk を用いたとしても、それを鍵 lk によって暗号化した暗号文が以前のものと変わるので、情報が漏れにくいという性質も有している。

【0277】ただし、図37の処理例においては、使用している暗号アルゴリズムが n ビットのもので、 r_1, r_2, r_3, sk のビット数も n ビットである時には、問題がある。もしソース機器が不正デバイスであった場合でも、ステップS300において、 Z の前半 n ビットとして、ステップS295で受信した Y の前半 n ビットをそのまま使うことにより、シンク機器のステップS303の検査をパスすることができてしまう。

【0278】この問題に鑑みて、ソース機器がシンク機器の正当性を確認した後にセッションキーを暗号化した暗号文を送信するのみならず、シンク機器がソース機器の正当性を確認できる認証プロトコルの処理例を図38から図40に示す。図38と図39の処理例は図37の処理例の変形例である。

【0279】図38に示した認証プロトコルの処理例を説明する。以下の処理例において、暗号化を行う際の暗号モードは、CBCモードなど、フィードバックを利用するものを使用する。

【0280】ステップS311からステップS327は図37のステップS281からステップS297と同様なので説明は省略する。ステップS328において、DVDプレーヤ1はあらかじめ定められたビット数（例えば64ビット）の乱数 r_4 とセッションキー sk を生成する。ステップS329において r_4 と r_3' と sk を連結して M_3 を作り、ステップS330において M_3 を鍵 lk で暗号化して Z を計算し、ステップS331において Z をパーソナルコンピュータ2に送信する。

【0281】ステップS332で Z を受信したパーソナルコンピュータ2は、ステップS333でこれを $license_key$ を用いて復号し、その結果をあらかじめ定められたビット数（例えば64ビット）ごとに分割して $r_4' || r_3'' || sk'$ とする。ステップS334で r_3'' が先に送信した r_3 と等しいかどうかを検査し、等しい場合のみ sk' をセッションキーとして受理する。

【0282】以上のように認証プロトコルを構成すれば、ソース機器がシンク機器の正当性を確認した後にセッションキーを暗号化した暗号文を送信するのみならず、シンク機器がソース機器の正当性を確認できる。

【0283】図39の処理例も図37の処理例の変形例である。以下の説明において、暗号化を行う際の暗号モードは、CBCモードなど、フィードバックを利用するものを使用する。

【0284】図39のステップS351からステップS361は図37のステップS281からステップS291と同様であるので説明は省略する。ステップS362において、パーソナルコンピュータ2はM2を $r2' || r3$ として生成する。ステップS363において、M2をlicense_keyで暗号化してYを得、ステップS364でDVDプレーヤ1に送信する。

【0285】ステップS365でYを受信したDVDプレーヤ1は、ステップS366でこれを鍵lkを用いて復号してその結果をあらかじめ定められたビット数（例えば64ビット）ごとに分割して $r2' || r3$ とおく。ステップS367において、 $r2'$ が先に送信した $r2$ と等しいかどうかを検査する。この検査に失敗した場合、DVDプレーヤ1はパーソナルコンピュータ2が正当な機器ではないと判断して認証プロトコルをそこで終了する。この検査に合格した場合、ステップS368においてDVDプレーヤ1はセッションキーskを生成し、ステップS369において、 $r3'$ とskを連結することによりM3を得る。ステップS370でM3を鍵lkを用いて暗号化して暗号文Zを得て、ステップS371でこれをパーソナルコンピュータ2に送信する。

【0286】パーソナルコンピュータ2はステップS372でZを受信し、ステップS373でZをlicense_keyで復号し、あらかじめ定められたビット数（例えば64ビット）ごとに分割して $r3' || sk'$ とする。ステップS374において、 $r3'$ が先に送信した $r3$ と等しいかどうかを検査する。この検査に失敗した場合、パーソナルコンピュータ2はDVDプレーヤ1が正当な機器ではないと判断して認証プロトコルを終了する。この検査に合格した場合、パーソナルコンピュータ2は sk' をセッションキーskとして受理する。

【0287】以上のように認証プロトコルを構成することにより、ソース機器はシンク機器が正当な機器であることを認証した後にセッションキーskを暗号化した暗号文をシンク機器に対して送ることができ、またシンク機器はソース機器が正当な機器であることを確認することができる。また本処理例では図33に示した処理例と同様に、たとえソース機器が以前使ったものと同じセッションキーskを用いたとしても、それを鍵lkによって暗号化した暗号文が以前のものと変わるので、情報が漏れにくいという性質も有している。

【0288】図40に示す認証プロトコルの処理例も同様の目的を満たすものである。以下の処理例において、暗号モードとしてはCBCモードなどのフィードバックを利用するものを使用するものとする。図40において、ステップS381からステップS384は図4のステップS1からステップS4と同様なので説明は省略する。ステップS385において、DVDプレーヤ1はあらかじめ定められたビット数（例えば64ビット）の乱数Rsrcを生成し、ステップS386でパーソナルコンピュータ

2に送信する。

【0289】ステップS387でパーソナルコンピュータ2はRsrcを受信し、ステップS388であらかじめ定められたビット数（例えば64ビット）の乱数Rsnkを生成し、ステップS389でRsnkとRsrcを連結してM1を生成し、ステップS390でM1を鍵license_keyを用いて暗号化してXを計算してステップS391でXを送信する。

【0290】DVDプレーヤ1はステップS392でXを受信し、ステップS393でパーソナルコンピュータ2のIDとservice_keyからlkを計算し、ステップS394でこのlkを用いてXを復号し、その結果をあらかじめ定められたビット数（例えば64ビット）ごとに分割して $Rsnk' || Rsrc'$ とする。ステップS395においてRsrc'が先に送信したRsrcと等しいことを検査し、この検査に合格しなければ、パーソナルコンピュータ2が不正デバイスであるとして認証プロトコルを終了する。この検査に合格すれば、DVDプレーヤ1はステップS396でセッションキーskを生成し、ステップS397でRsrcとRsnk'とskを連結してM2を生成し、ステップS398でM2を鍵lkを用いて暗号化してYを得、ステップS399でパーソナルコンピュータ2に送信する。

【0291】ステップS400でYを受信したパーソナルコンピュータ2は、ステップS401で鍵license_keyを用いてYを復号してこの結果をあらかじめ定められたビット数（例えば64ビット）ごとに分割して $Rsrc' || Rsnk' || sk'$ とおく。ステップS402でRsnk'が先に送信したRsnkと等しいことを検査する。この検査に失敗した場合、パーソナルコンピュータ2は、DVDプレーヤ1が不正デバイスであるとして sk' を破棄する。この検査に合格した場合には、パーソナルコンピュータ2はDVDプレーヤ1が正当なデバイスであることを認め、 sk' をセッションキーとして受理する。

【0292】以上のように認証プロトコルを構成することにより、ソース機器はシンク機器が正当な機器であることを認証した後にセッションキーskを暗号化した暗号文をシンク機器に対して送ることができ、またシンク機器はソース機器が正当な機器であることを確認することができる。また本処理例では図33に示した処理例と同様に、たとえソース機器が以前使ったものと同じセッションキーskを用いたとしても、それを鍵lkによって暗号化した暗号文が以前のものと変わるので、情報が漏れにくいという性質も有している。

【0293】以上においては、DVDプレーヤ1をソースとし、パーソナルコンピュータ2と光磁気ディスク装置3をシンクとしたが、いずれの装置をソースとするかシンクとするかは任意である。

【0294】また、各電子機器を接続する外部バスも、1394バスに限らず、種々のバスを利用することができ、それに接続する電子機器も、上述した例に限らず、

任意の装置とすることができる。

【0295】なお、上記各種の指令を実行するプログラムは、磁気ディスク、CD-ROMディスクなどの提供媒体を介してユーザに提供したり、ネットワークなどの提供媒体を介してユーザに提供し、必要に応じて内蔵するRAMやハードディスクなどに記憶して利用させるようにすることができる。

【0296】

【発明の効果】以上の如く、請求項1に記載の情報処理装置、請求項7に記載の情報処理方法、および請求項13に記載の提供媒体によれば、第1のキーLKを、識別データと、所定の処理を施す情報に対応する第2のキーSVKに基づいて生成するようにしたので、安全性を向上することが可能となる。

【0297】請求項14に記載の情報処理装置、請求項18に記載の情報処理方法、および請求項19に記載の提供媒体によれば、他の情報処理装置からの識別データと第1のキーSVKに対して関数を適用して、第2のキーLKを生成し、第2のキーLKを用いて、第3のキーSKを暗号化し、他の情報処理装置に伝送するようにしたので、より安全に、適正な他の情報処理装置に対してだけ、所定の情報処理を行わせるようにすることが可能となる。

【0298】請求項20に記載の情報処理システム、請求項21に記載の情報処理方法、および請求項22に記載の提供媒体によれば、第2の情報処理装置の識別データと第1のキーSVKに対して関数を適用して第2のキーLK1生成し、第2のキーLK1を用いて第3のキーSK1を暗号化して、第2の情報処理装置に伝送し、第2の情報処理装置において、記憶している第4のキーLK2を用いて、暗号化されている第3のキーSK1を復号するようにしたので、より安全性の高い情報処理システムを実現することができる。

【0299】請求項23に記載の情報処理装置、請求項27に記載の情報処理方法、および請求項28に記載の提供媒体によれば、第2のキーLK'を、第1のキーLKと、関数Gの逆関数 G^{-1} に基づいて生成するようにしたので、より安全性を高めることができる。

【0300】請求項29に記載の情報処理装置、請求項30に記載の情報処理方法、および請求項31に記載の提供媒体によれば、他の情報処理装置の識別データと第1のキーSVKに対して関数を適用して得られるデータHから得られる疑似乱数pRNG(H)を用いて、第2のキーSKを暗号化して、他の情報処理装置に伝送するようにしたので、より安全な情報処理装置を実現することができる。

【0301】請求項32に記載の情報処理システム、請求項33に記載の情報処理方法、および請求項34に記載の提供媒体によれば、第1の情報処理装置において、第2の情報処理装置の識別データと、第1のキーSVKに対して関数hを適用して得られるデータHから生成した

疑似乱数pRNG(H)を用いて、第2のキーSKを暗号化して、第2の情報処理装置に伝送し、第2の情報処理装置において、第4のキーLK'を、第3のキーLKと、関数Gの逆関数 G^{-1} に基づいて生成するようにしたので、より安全な情報処理システムを実現することが可能となる。

【図面の簡単な説明】

【図1】本発明を適用した情報処理システムの構成例を示すブロック図である。

【図2】図1のDVDプレーヤ1、パーソナルコンピュータ2、および光磁気ディスク装置3の内部の構成例を示すブロック図である。

【図3】認証処理を説明する図である。

【図4】認証処理を説明するタイミングチャートである。

【図5】node_unique_IDのフォーマットを示す図である。

【図6】他の認証処理を説明するタイミングチャートである。

【図7】さらに他の認証処理を説明するタイミングチャートである。

【図8】他の認証処理を説明するタイミングチャートである。

【図9】他の認証処理を説明するタイミングチャートである。

【図10】暗号化処理を説明するブロック図である。

【図11】図10の1394インタフェース26の構成例を示すブロック図である。

【図12】図11の1394インタフェース26のより詳細な構成例を示すブロック図である。

【図13】図12のLFSR72のより詳細な構成例を示すブロック図である。

【図14】図13のLFSR72のより具体的な構成例を示すブロック図である。

【図15】図10の1394インタフェース36の構成例を示すブロック図である。

【図16】図15の1394インタフェース36のより詳細な構成例を示すブロック図である。

【図17】図10の1394インタフェース49の構成例を示すブロック図である。

【図18】図17の1394インタフェース49のより詳細な構成例を示すブロック図である。

【図19】図10のアプリケーション部61の構成例を示すブロック図である。

【図20】図19のアプリケーション部61のより詳細な構成例を示すブロック図である。

【図21】図10の1394インタフェース26の他の構成例を示すブロック図である。

【図22】図10の1394インタフェース36の他の構成例を示すブロック図である。

【図23】図10の1394インタフェース49の他の構成例を示すブロック図である。

【図24】図10のアプリケーション部61の他の構成例を示すブロック図である。

【図25】他の認証処理を説明するタイミングチャートである。

【図26】図25に続くタイミングチャートである。

【図27】図25に続く他のタイミングチャートである。

【図28】本発明の情報処理システムの他の構成例を示すブロック図である。

【図29】図28の乱数発生器903の構成例を示すブロック図である。

【図30】図28の演算回路902の処理を説明するフローチャートである。

【図31】他の認証処理を説明するタイミングチャートである。

【図32】パケットフォーマットを示す図である。

【図33】他の認証処理を説明するタイミングチャートである。

【図34】CBCモードの構成例を示すブロック図である。

【図35】他の認証処理を説明するタイミングチャートである。

【図36】他の認証処理を説明するタイミングチャートである。

【図37】他の認証処理を説明するタイミングチャートである。

【図38】他の認証処理を説明するタイミングチャートである。

【図39】他の認証処理を説明するタイミングチャートである。

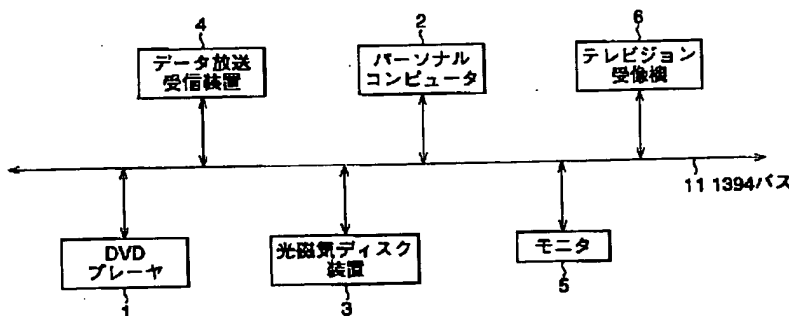
【図40】他の認証処理を説明するタイミングチャートである。

【図41】従来の認証方法を説明するタイミングチャートである。

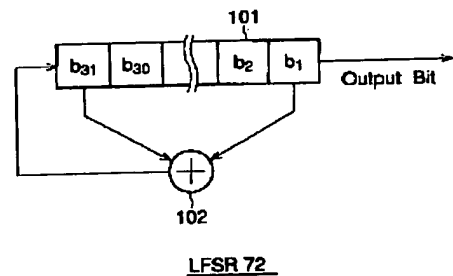
【符号の説明】

1 DVDプレーヤ, 2 パーソナルコンピュータ,
3 光磁気ディスク装置, 11 1394バス, 2
0 ファームウェア, 21 CPU, 25 ドライブ,
26 1394インタフェース, 27 EEPROM,
31 CPU, 35 ドライブ, 36 1394インタ
フェース, 37 EEPROM, 41 CPU, 47 ハー
ドディスク, 48 拡張ボード, 49 1394イ
ンタフェース, 50 EEPROM, 51 内部バス,
61 アプリケーション部, 62 ライセンスマネー
ジャ

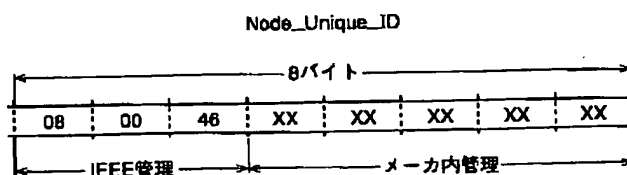
【図1】



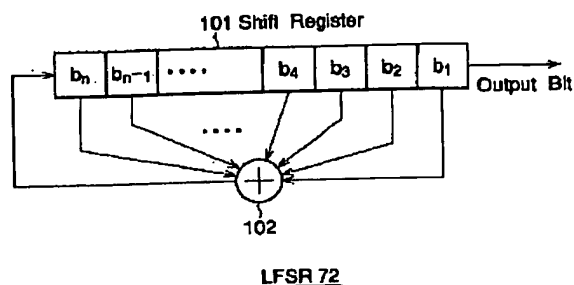
【図14】



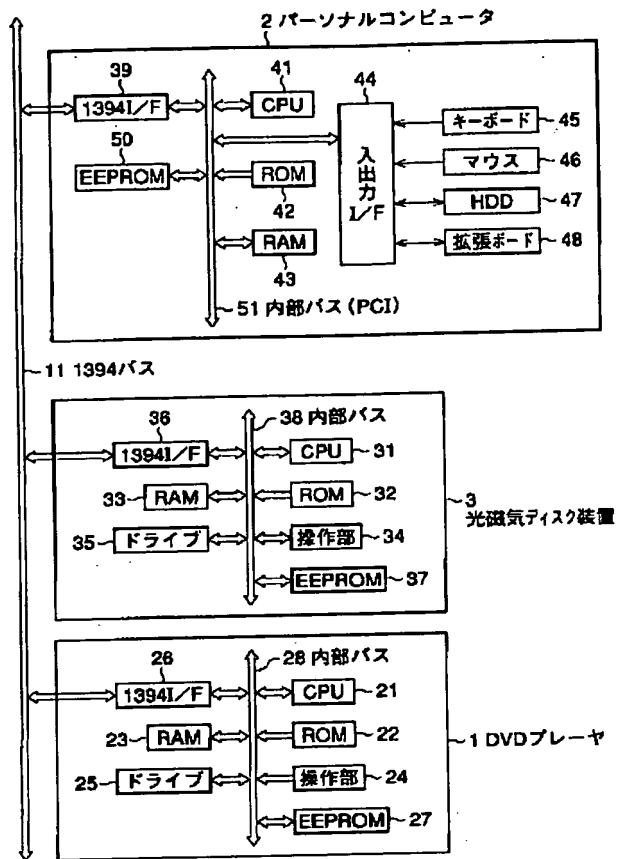
【図5】



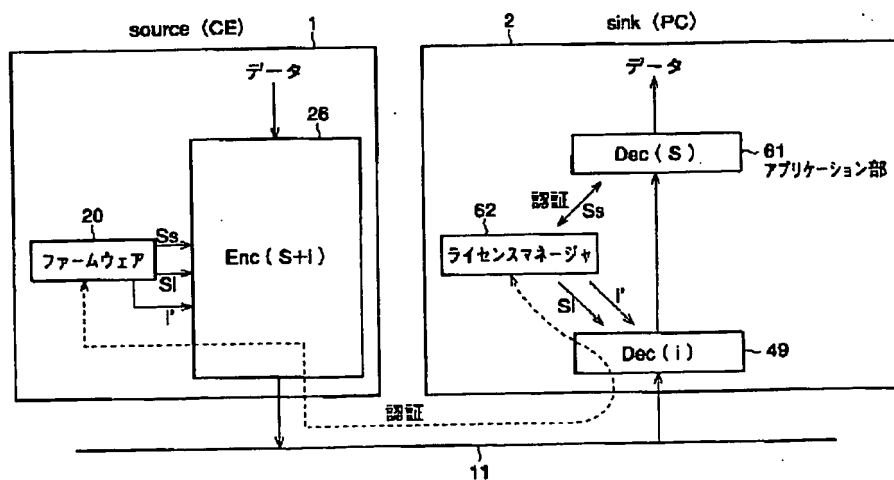
【図13】



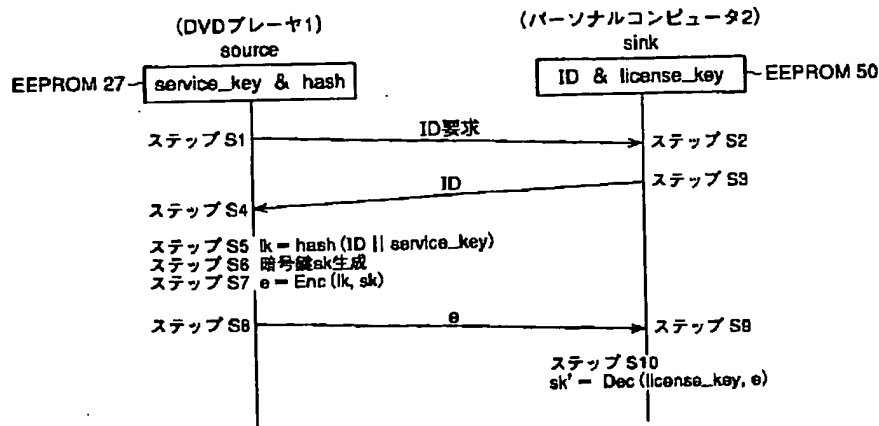
【図2】



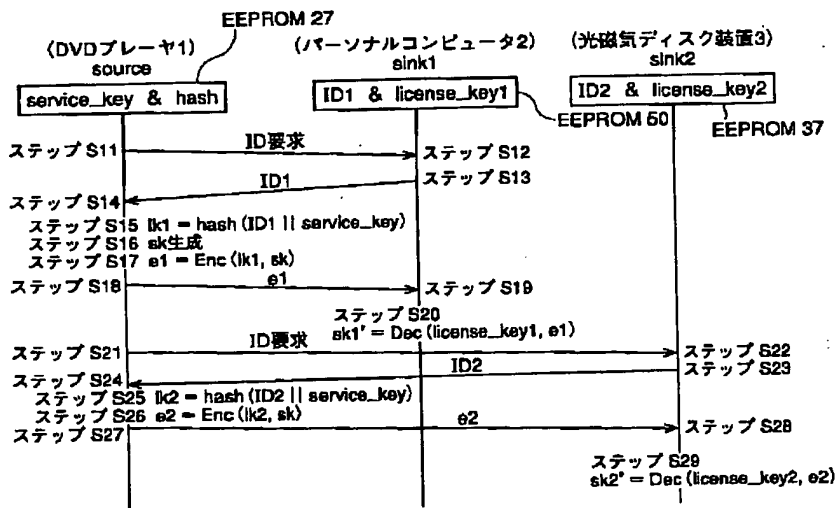
【図3】



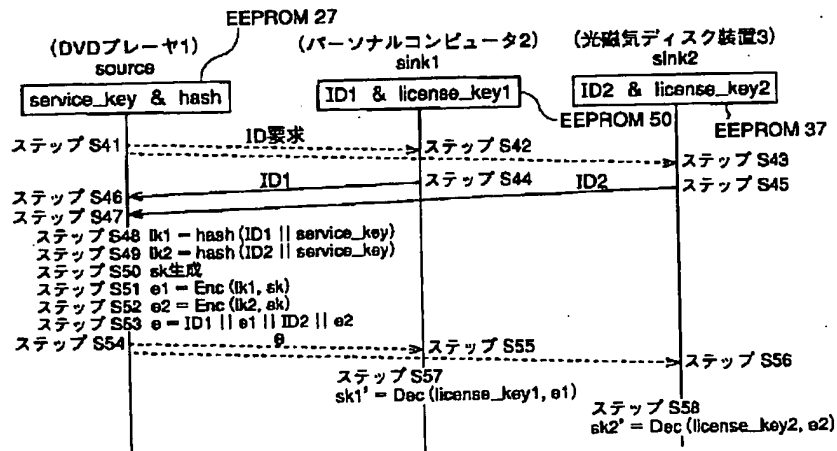
【図4】



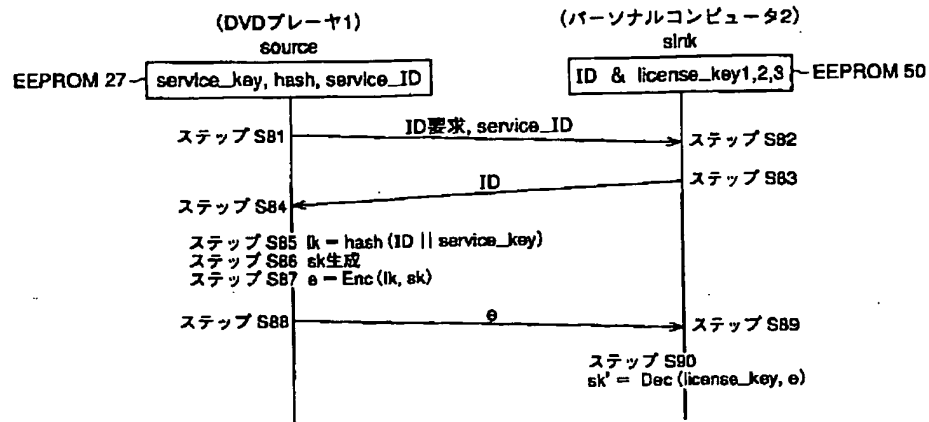
【図6】



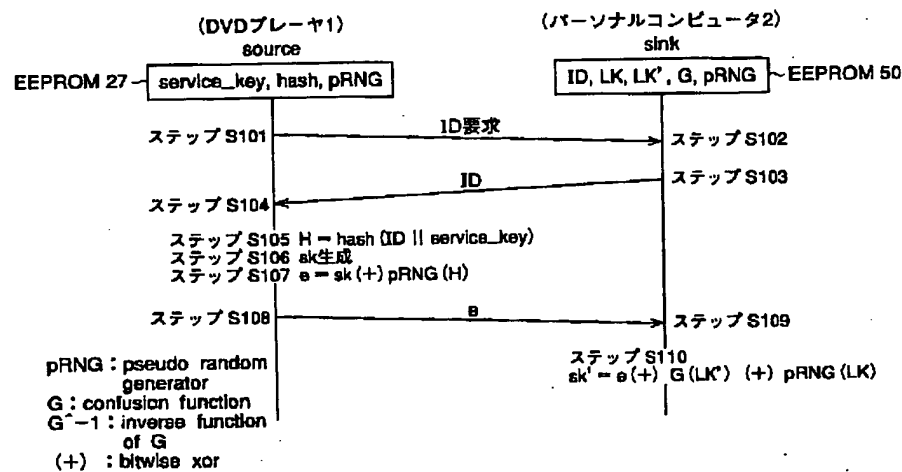
【図7】



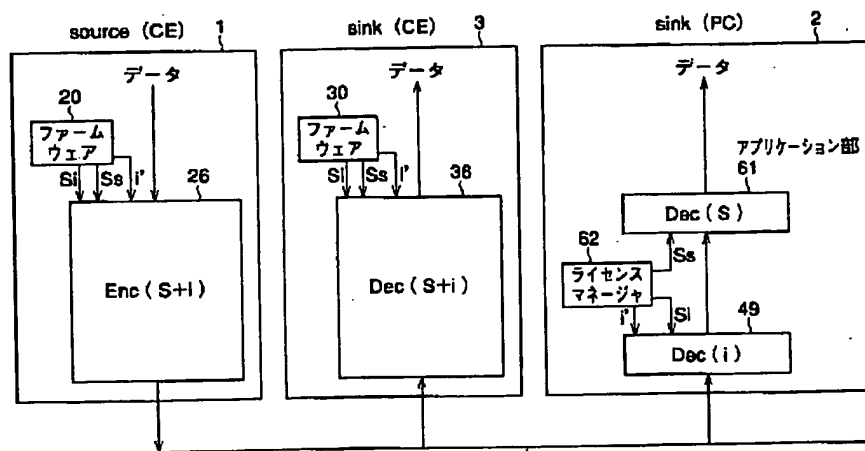
【図8】



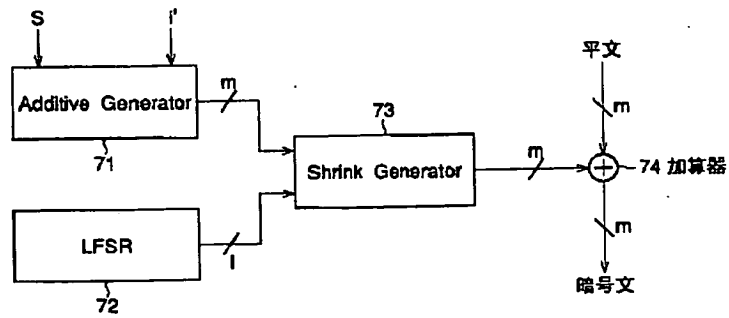
【図9】



【図10】

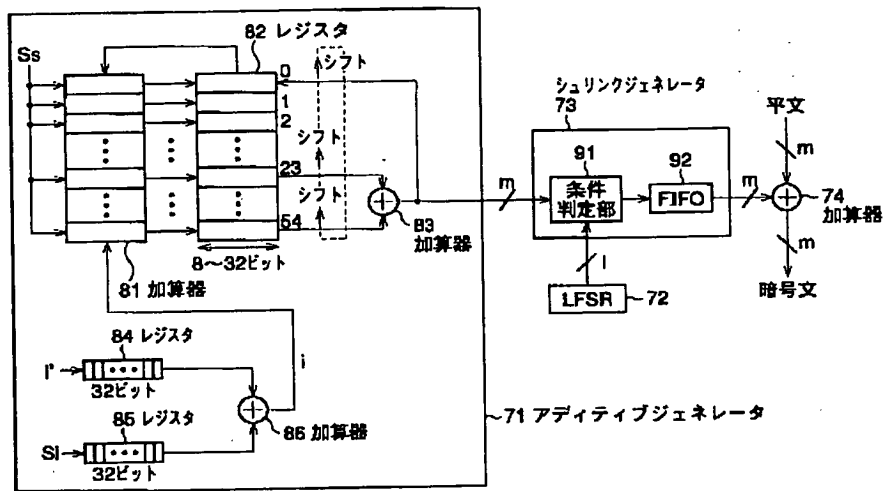


【図11】



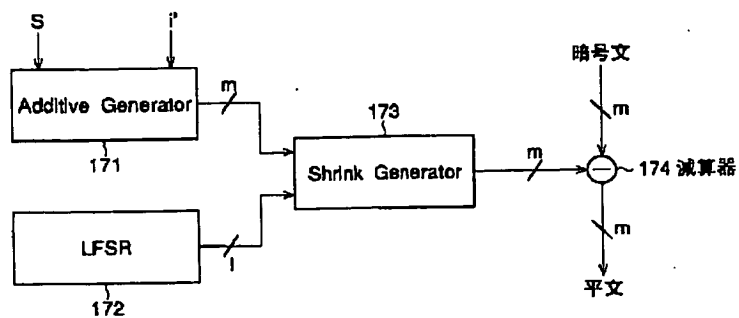
13941/F 26
(ソース (CE))

【図12】



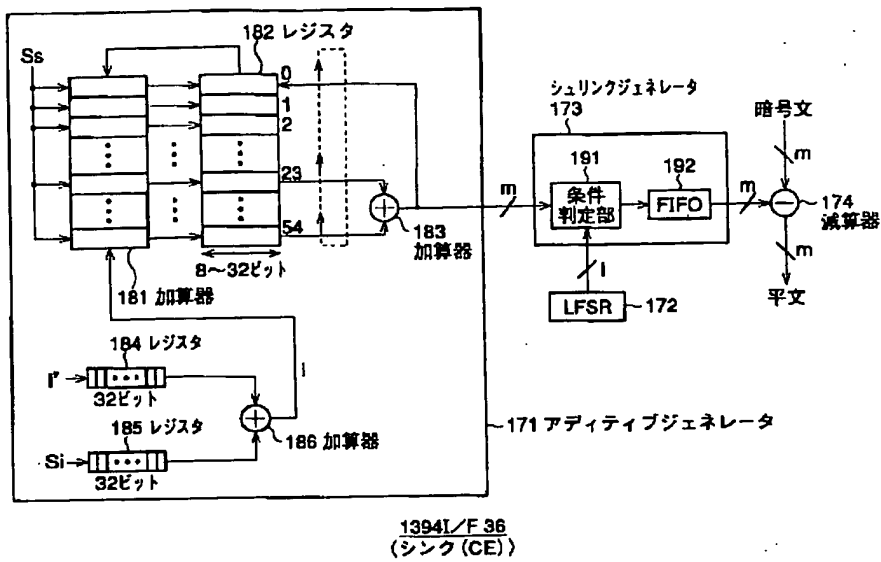
13941/F 26
(ソース (CE))

【図15】

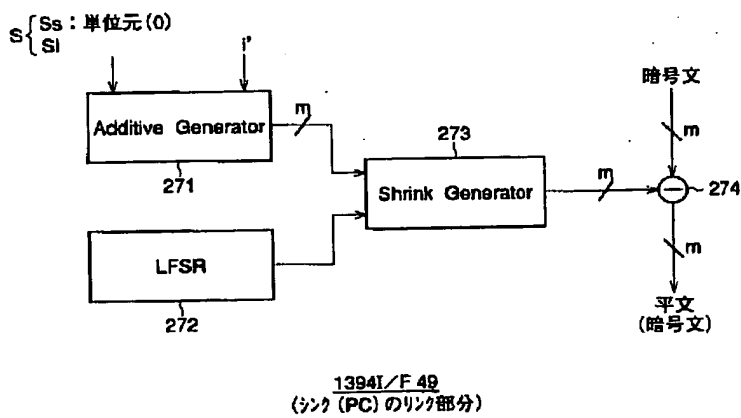


13941/F 36
(シンク (CE))

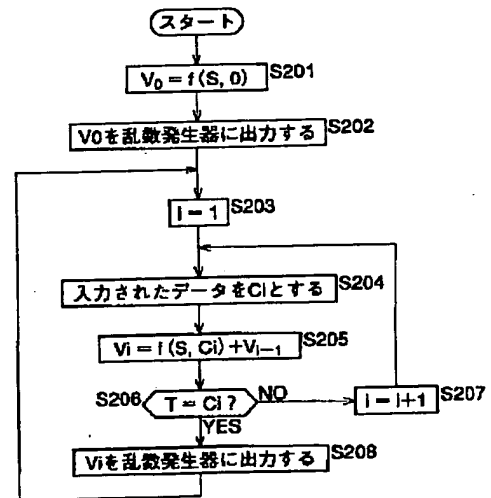
【図16】



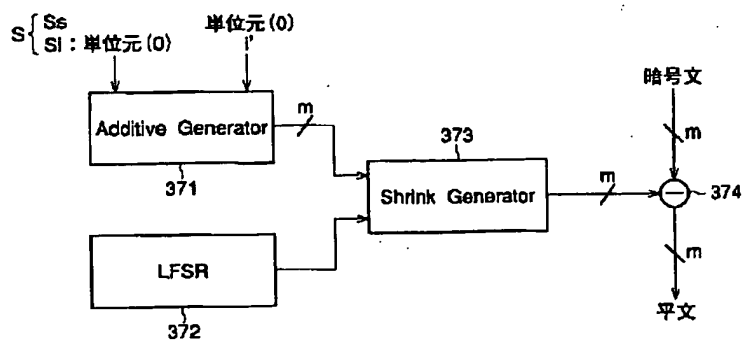
【図17】



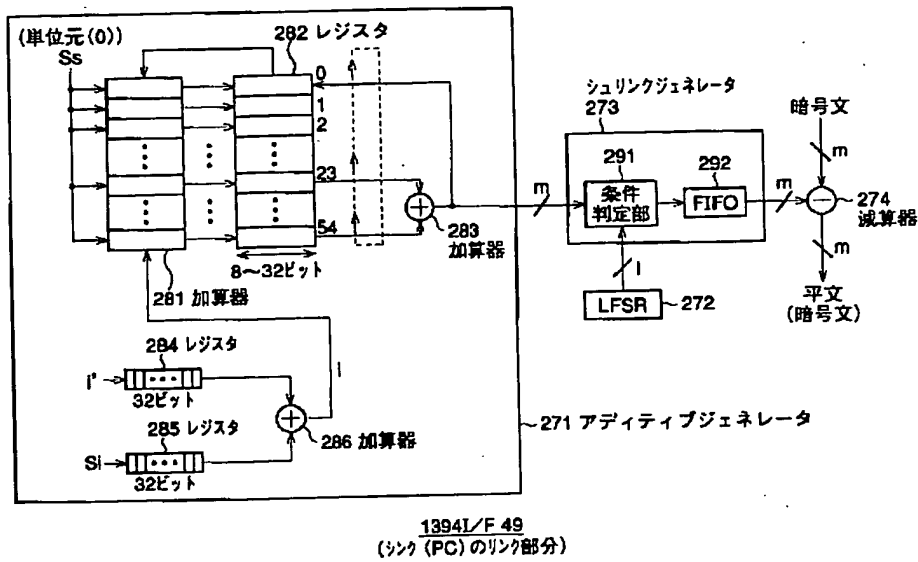
【図30】



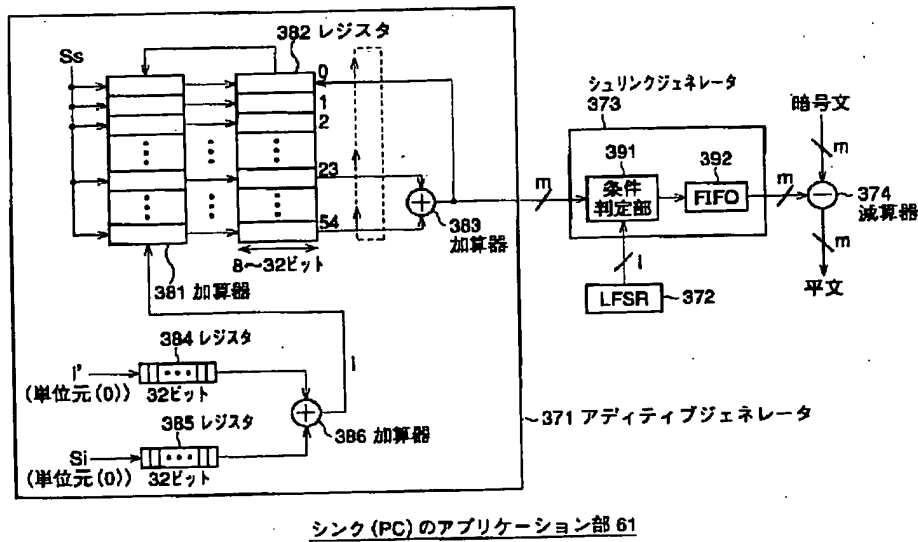
【図19】



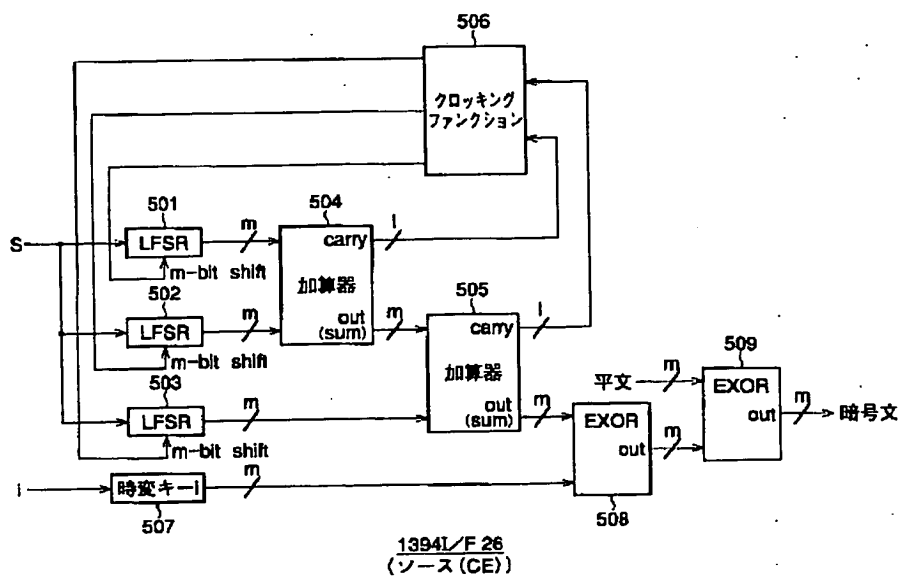
【図18】



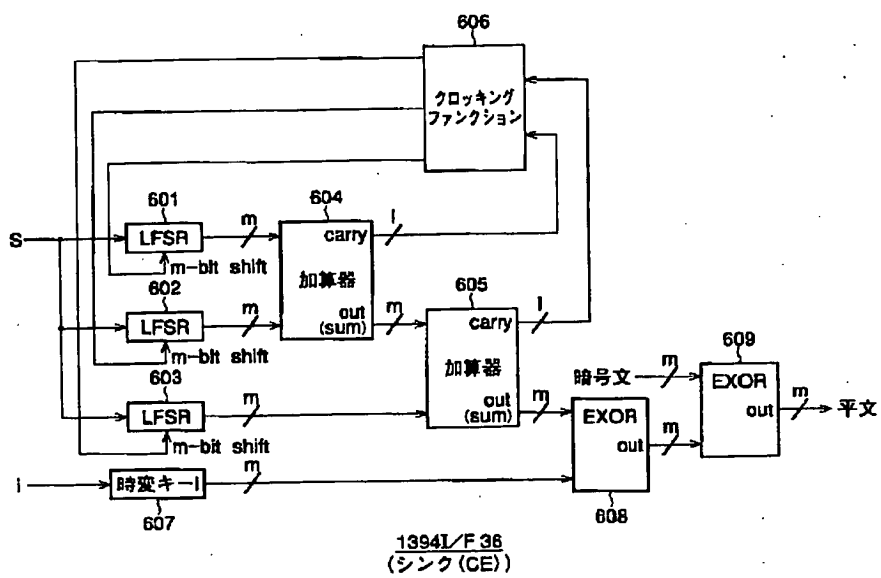
【図20】



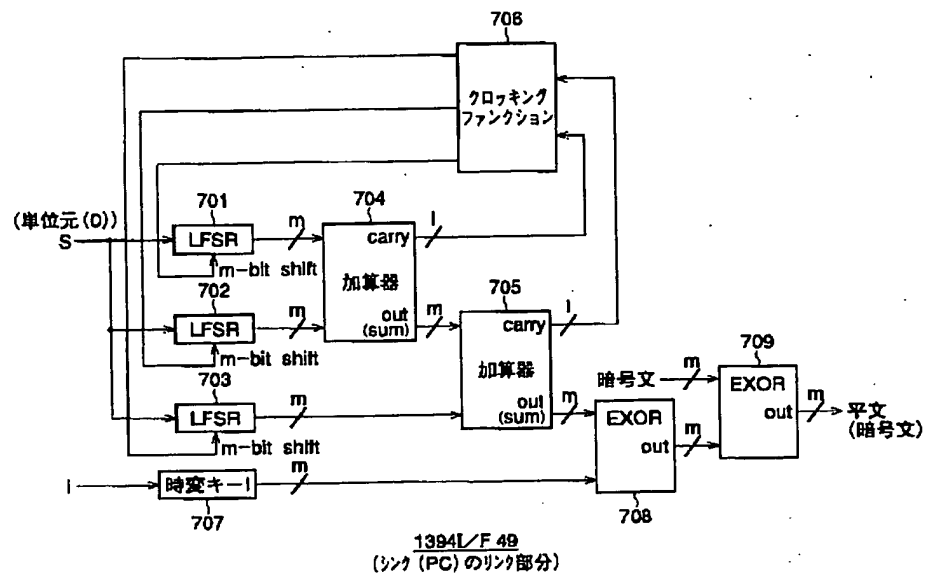
【図21】



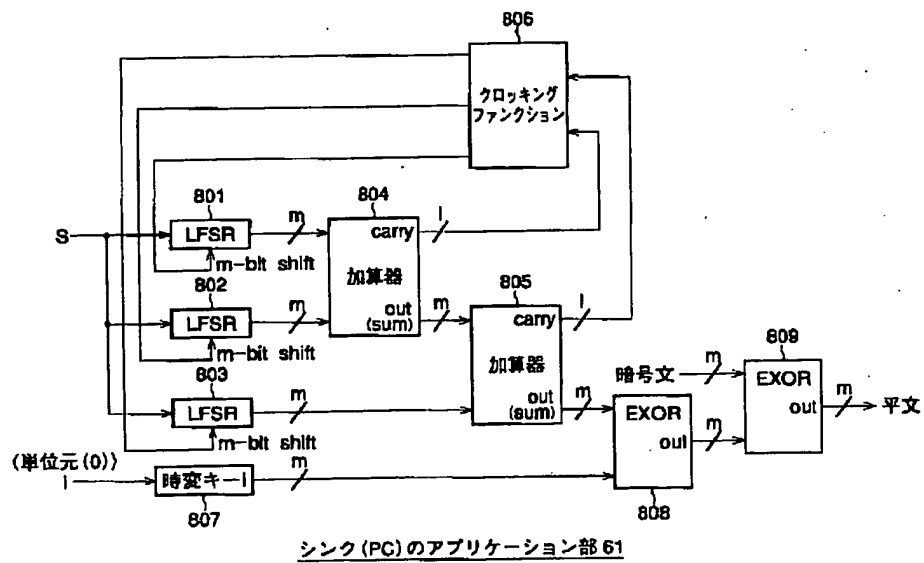
【図22】



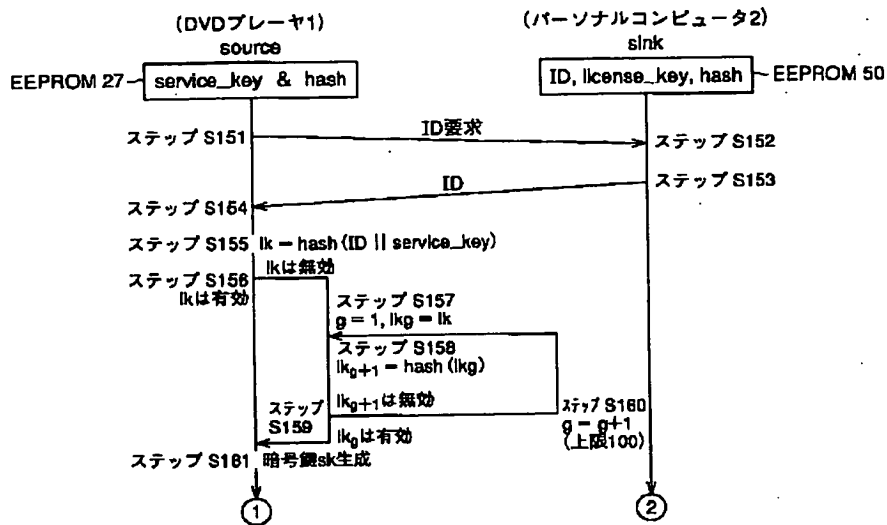
【図23】



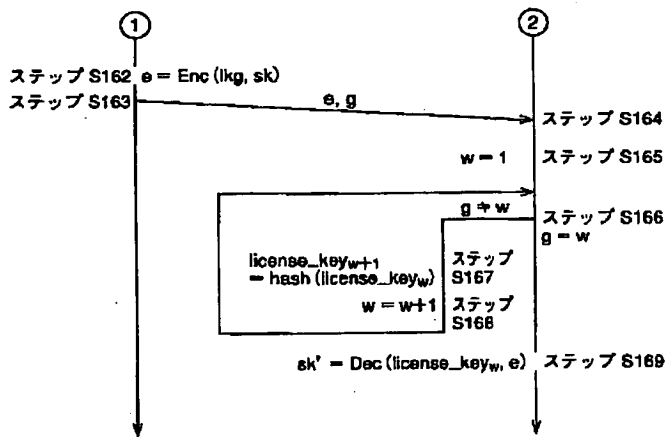
【図24】



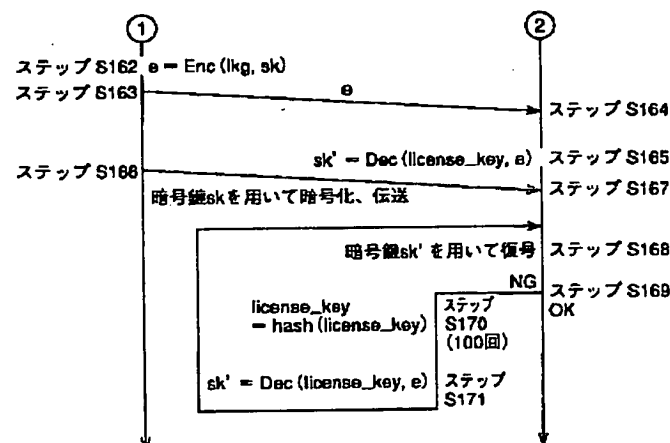
【図25】



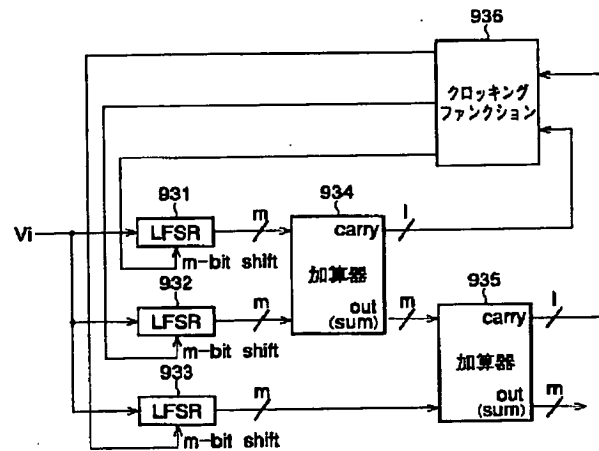
【図26】



【図27】

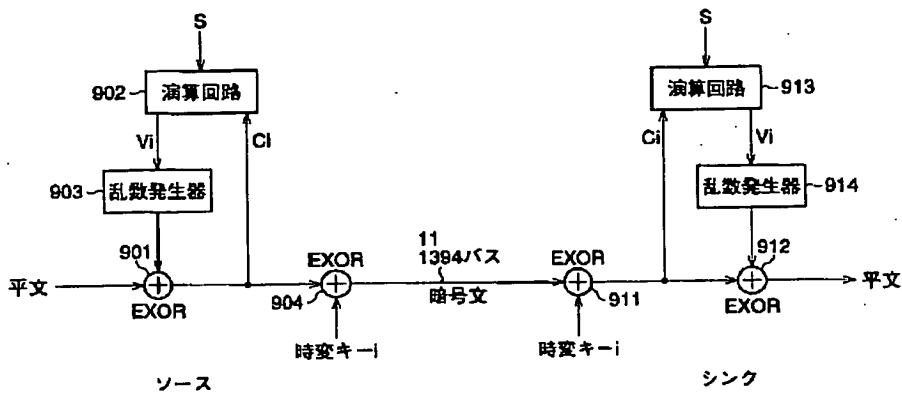


【図29】

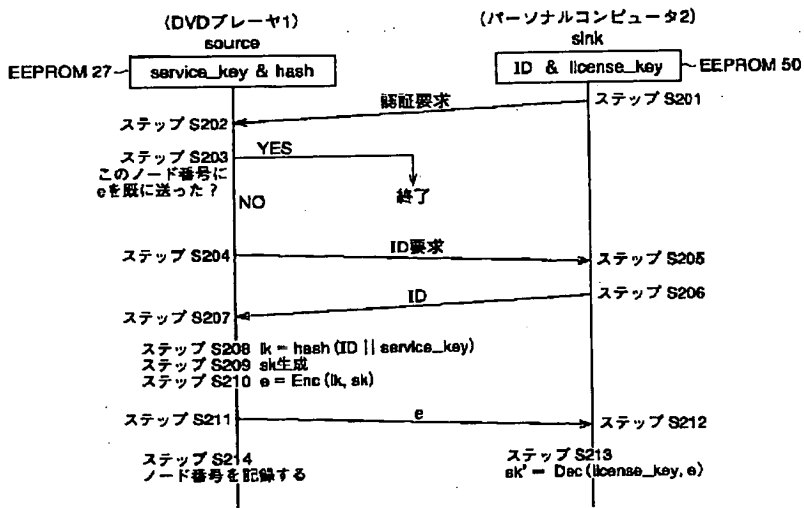


乱数発生器 903 (914)

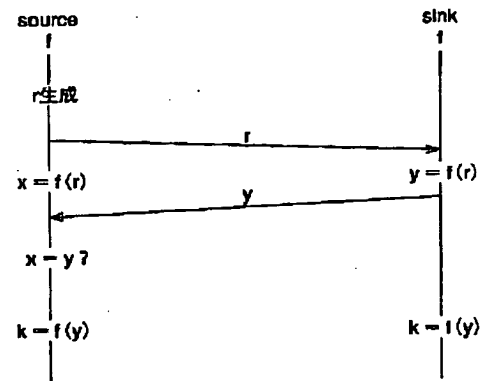
【図28】



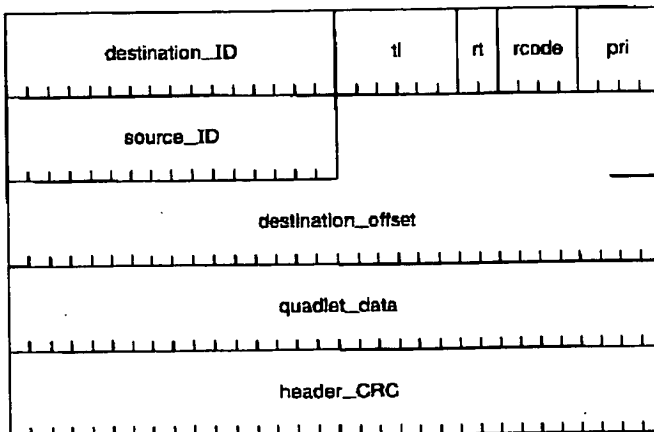
【図31】



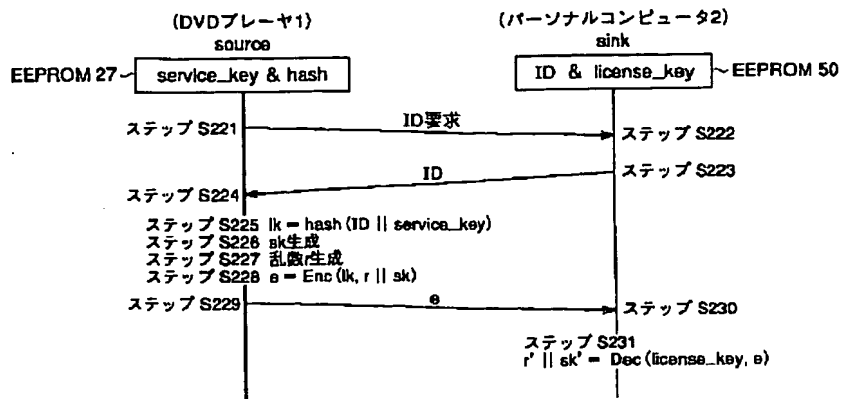
【図41】



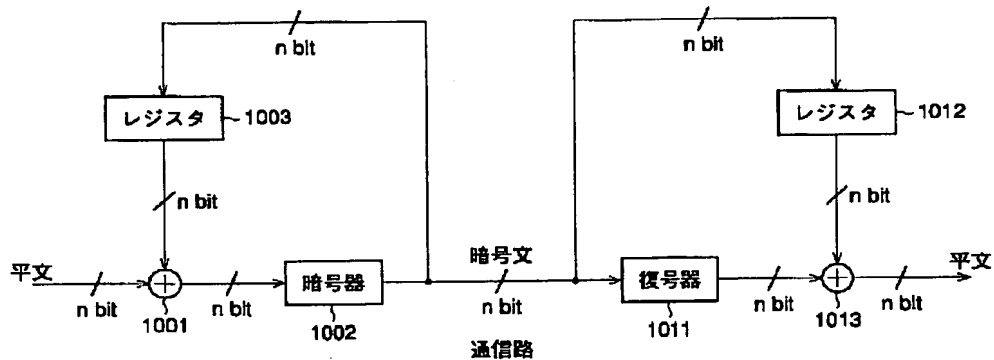
【図32】



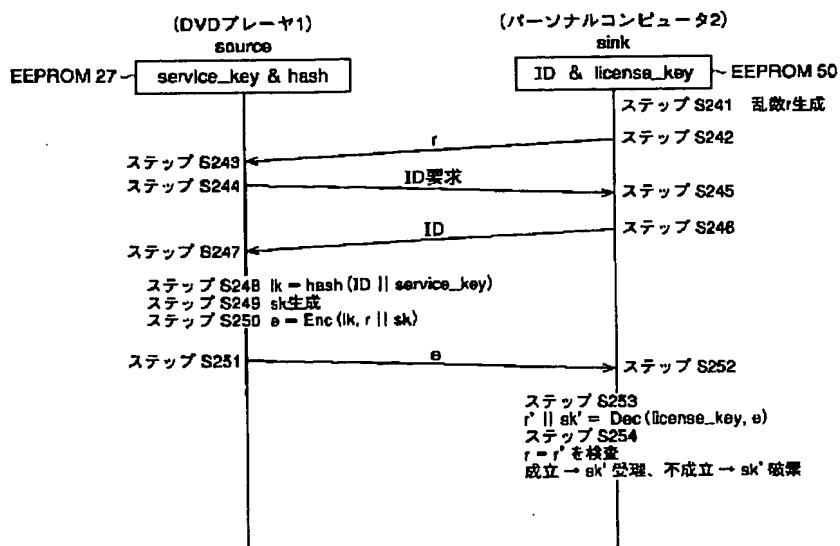
【図33】



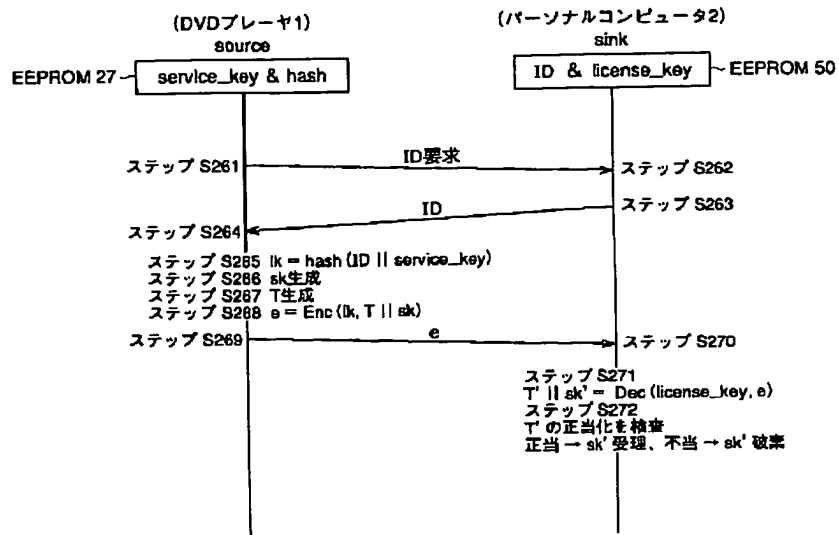
【図34】



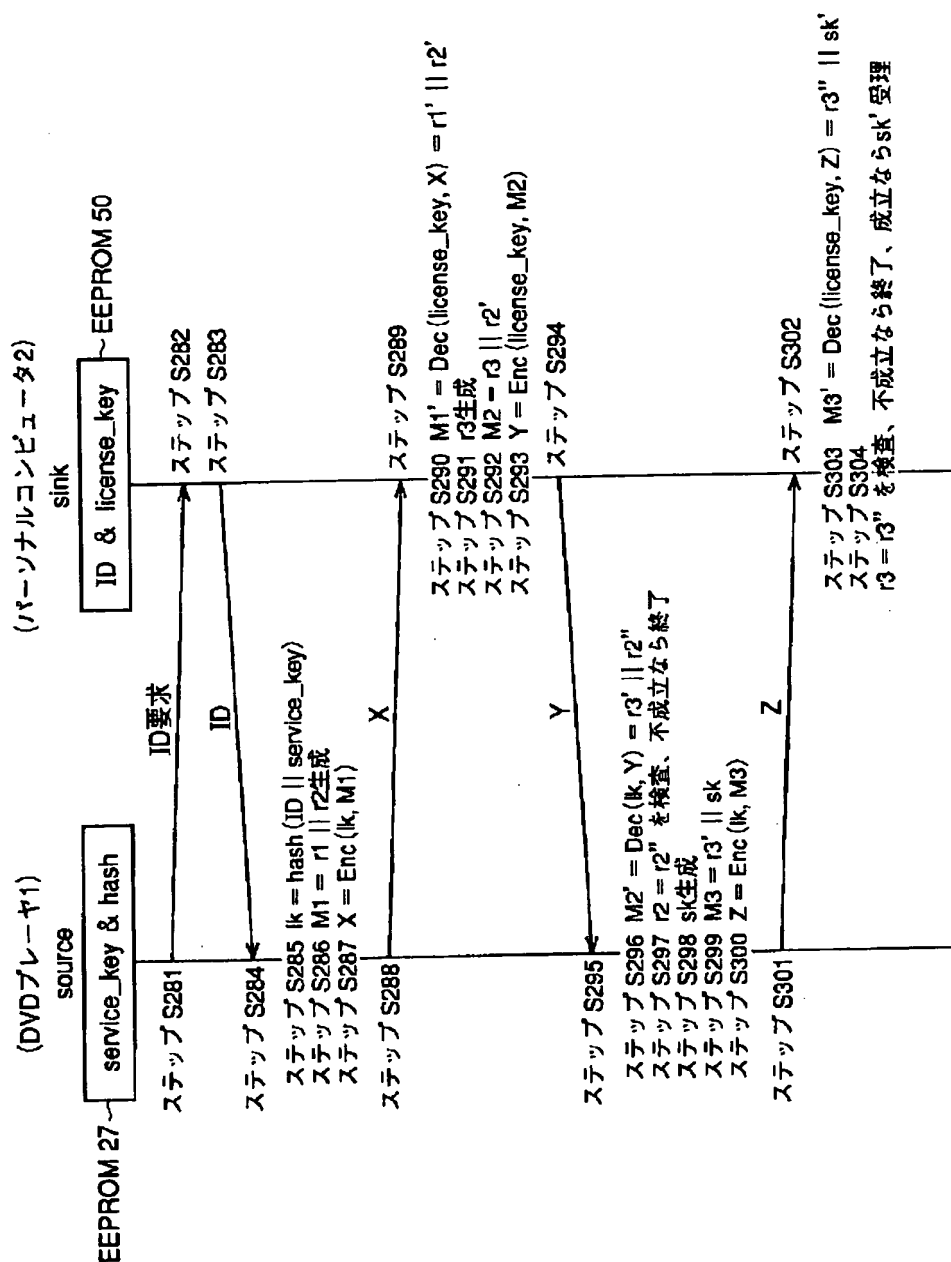
【図35】



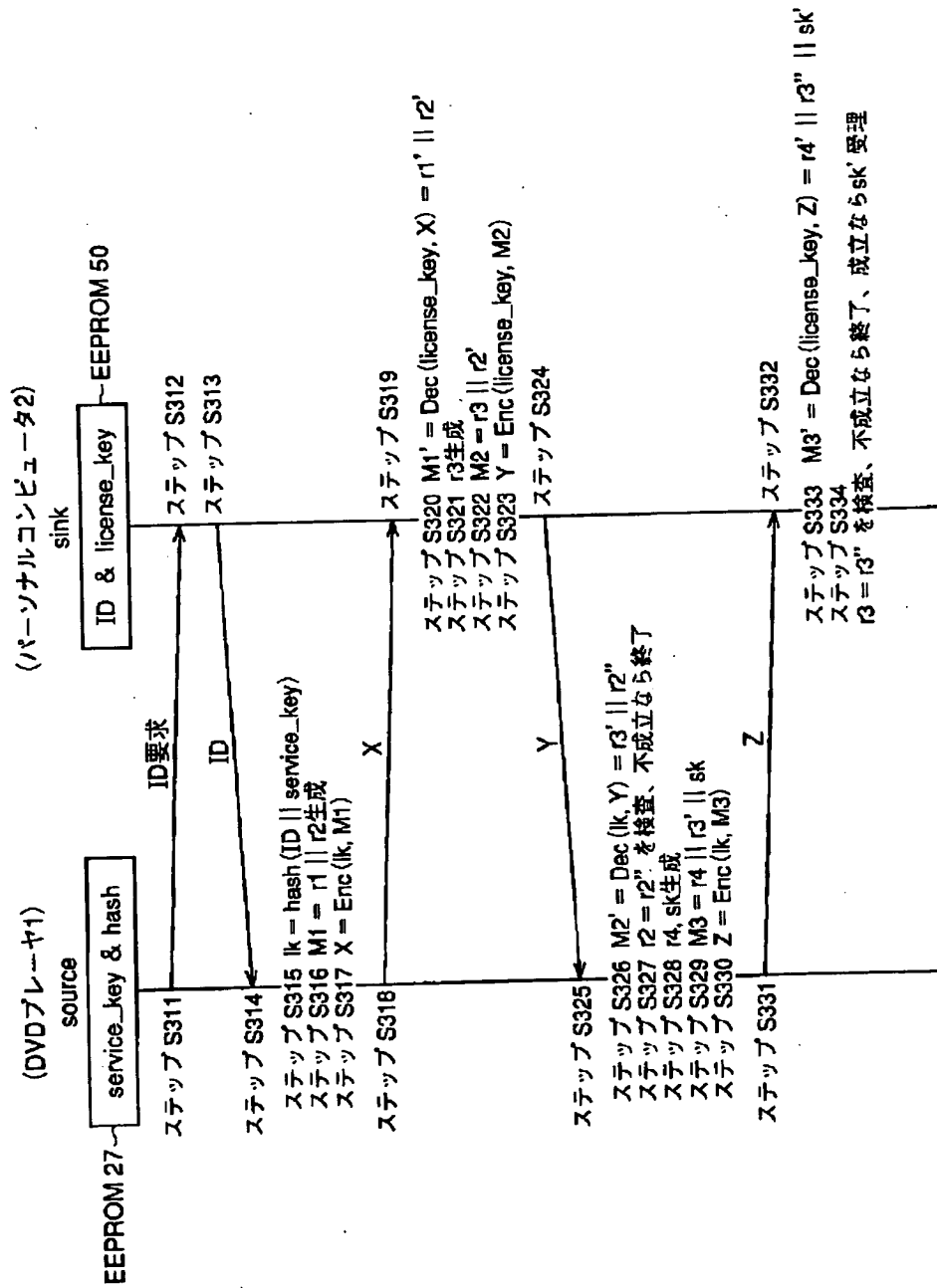
【図36】



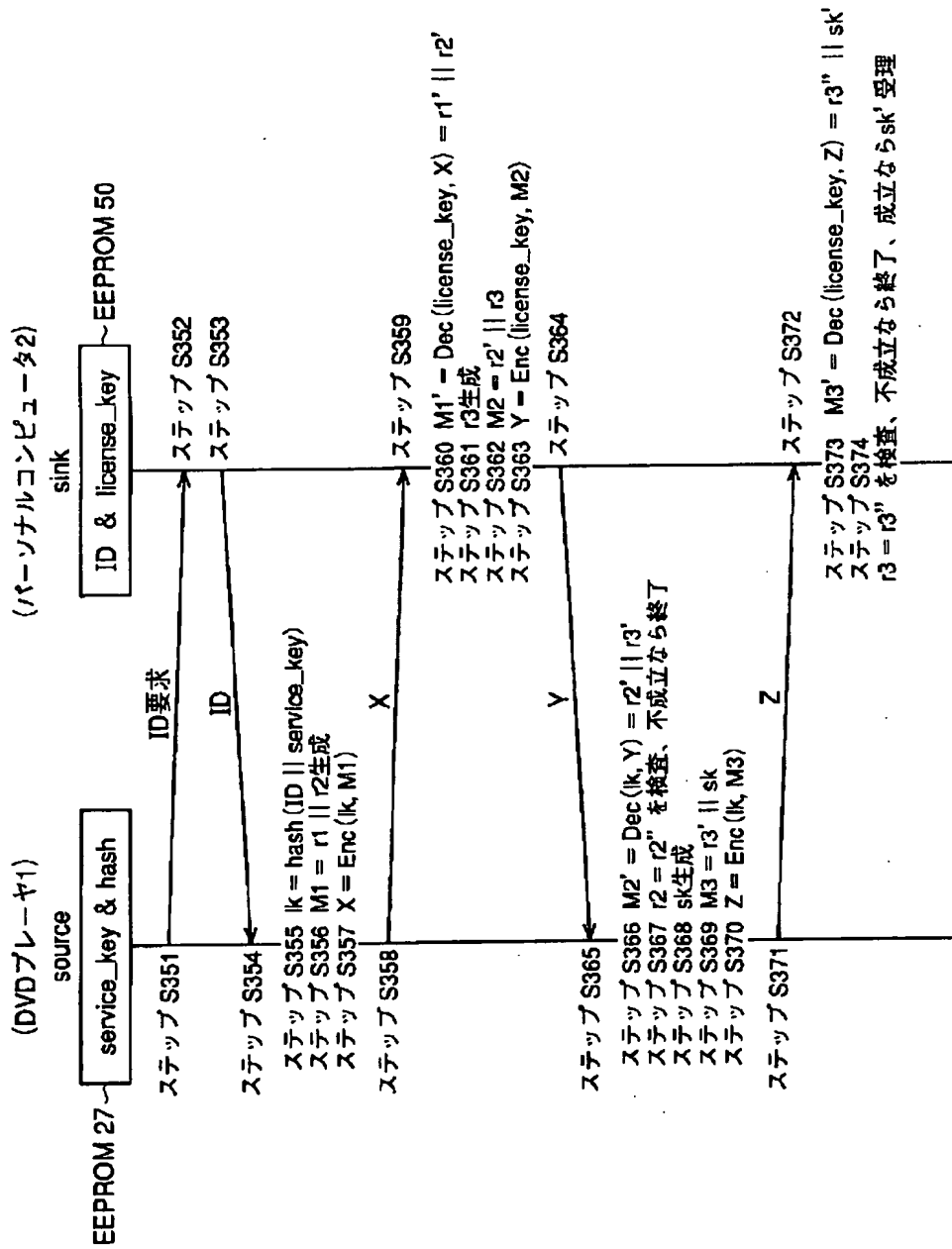
【図37】



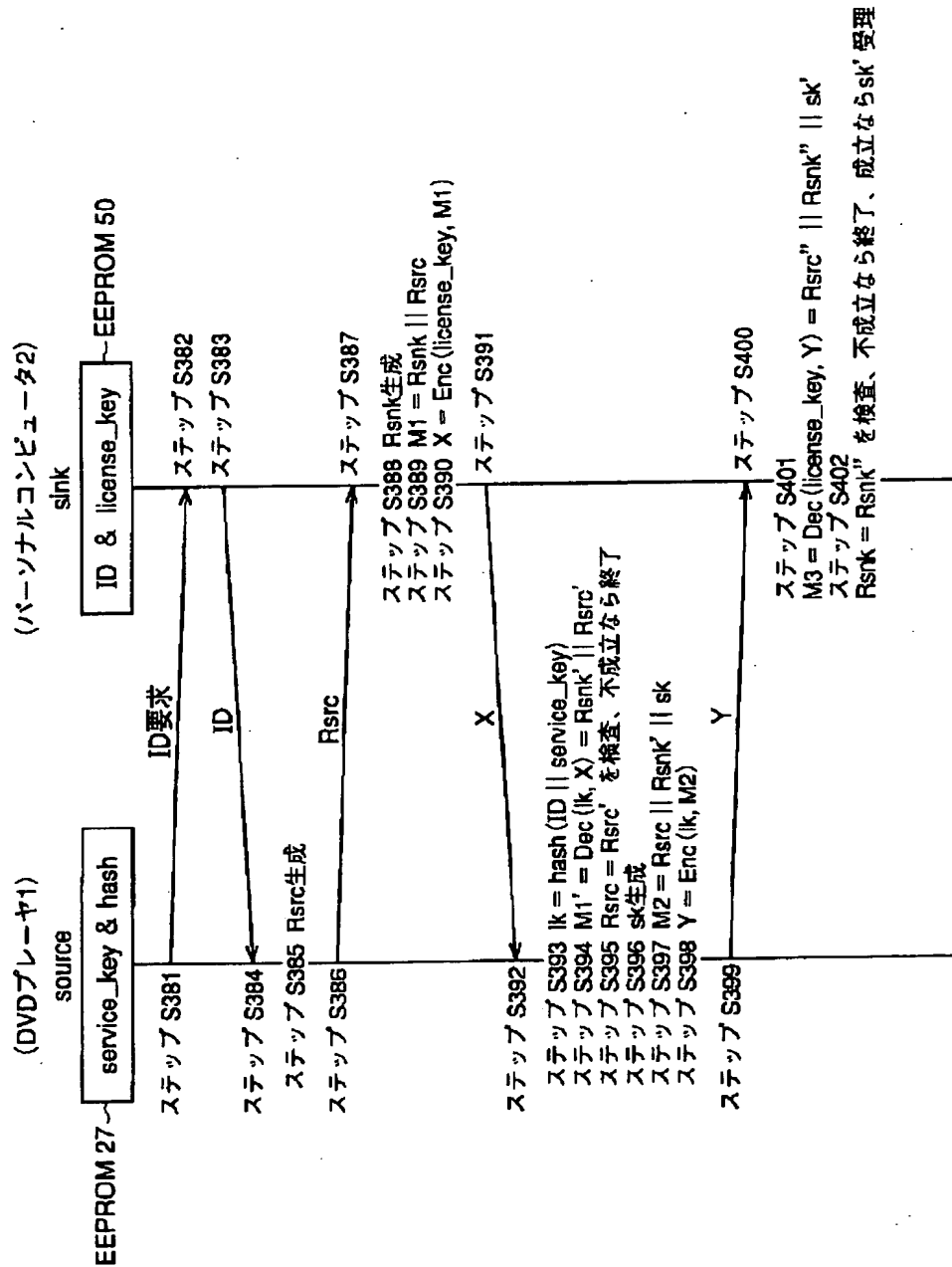
【図38】



【図39】



【図40】



フロントページの続き

(72)発明者 佐藤 真
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(72)発明者 嶋 久登
アメリカ合衆国 カリフォルニア州 サラ
トガ バセオ・フローレス12610

(72)発明者 中野 雄彦
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内

(72)発明者 浅野 智之
東京都品川区北品川6丁目7番35号 ソニ
ー株式会社内